

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: )  
Kazushi ISHIGAKI )  
Serial No.: Not Yet Assigned )  
Filed: December 22, 2000 )



For: ELECTRONIC COMMERCE SYSTEM AND METHOD

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

*Assistant Commissioner for Patents*  
*Washington, D.C. 20231*


*Sir:*

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s)  
herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-191300  
Filed: June 26, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing  
date as evidenced by the certified papers attached hereto, in accordance with the requirements  
of 35 U.S.C. §119.

Respectfully submitted,  
STAAS & HALSEY LLP

By:   
H.J. Staas  
Registration No. 22,010

700 11th Street, N.W., Ste. 500  
Washington, D.C. 20001  
(202) 434-1500  
Date: Dec. 22, 2000

日本国特許庁

PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年 6月26日

出願番号

Application Number:

特願2000-191300

出願人

Applicant(s):

富士通株式会社

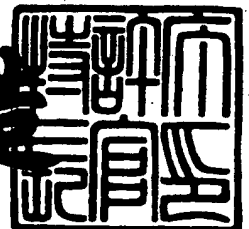


CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年11月 6日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2000-3090370

【書類名】 特許願

【整理番号】 0095142

【提出日】 平成12年 6月26日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明の名称】 電子商取引システムおよび電子商取引方法

【請求項の数】 20

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 石垣 一司

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100095555

【弁理士】

【氏名又は名称】 池内 寛幸

【電話番号】 06-6361-9334

【手数料の表示】

【予納台帳番号】 012162

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9803089

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子商取引システムおよび電子商取引方法

【特許請求の範囲】

【請求項 1】 利用者と業者の間の商取引を扱う電子商取引システムであって

業者端末が備える、利用者が提示した利用者識別情報を読み取る利用者識別情報読み取り部と、

前記業者端末が備える、前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

前記業者端末が備える、提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る手書きサイン入力部と、

第 3 者機関が備える、前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と電子サインデータを取得し、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する電子透かし付与部と、

前記業者端末が備える、前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する商取引データ格納部とを備えたことを特徴とした電子商取引システム。

【請求項 2】 利用者と業者の間の商取引を扱う電子商取引システムであって

業者端末が備える、利用者が提示した利用者識別情報を読み取る利用者識別情報読み取り部と、

前記利用者端末が備える、前記業者端末から取得した前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

利用者端末が備える、提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る手書きサイン入力部と、

第 3 者機関が備える、前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と前記利用者端末からの電子サインデータとを取得し、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報とし

て付与し、電子透かし付き電子サインデータを生成する電子透かし付与部と、

前記業者端末が備える、前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する商取引データ格納部とを備えたことを特徴とした電子商取引システム。

【請求項3】 利用者と業者の間の商取引を扱う電子商取引システムであって、

業者端末が備える、利用者が提示した利用者識別情報を読み取る利用者識別情報読み取り部と、

前記利用者端末が備える、前記業者端末から取得した前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

利用者端末が備える、提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る手書きサイン入力部と、

前記利用者端末が備える、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する電子透かし付与部と、

前記業者端末が備える、前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する商取引データ格納部とを備えたことを特徴とした電子商取引システム。

【請求項4】 前記第3者機関が、前記利用者識別情報を基に予め登録されている前記利用者の真正サインデータを検索し、該真正サインデータを用いて前記電子サインデータの照合・認証を行うサイン認証部を備えた請求項1～3のいずれかに記載の電子商取引システム。

【請求項5】 前記電子透かし付与部が、前記電子サインデータを予め指定されたビット長の電子データに要約した要約情報を生成する電子サインデータ要約部を備え、前記商取引識別子に加えて前記要約情報も電子透かし情報として前記電子サインデータに対して付与する請求項1～4のいずれかに記載の電子商取引システム。

【請求項6】 前記電子透かし付与部は、前記業者端末を介した電子サインデータの送信があった場合に、登録されている利用者の連絡先データを基に利用者

に対して直接、該商取引における電子透かし付き電子サインデータ生成是非の確認を行う利用者確認部を備え、

前記利用者確認部は、前記利用者からの確認が得られない場合には前記業者端末に対して前記電子透かし付き電子サインデータの生成の拒否を通知する請求項 1 に記載の電子商取引システム。

【請求項 7】 前記電子透かし付与部が電話通信手段と音声応答システムを備え、前記利用者の連絡先データが利用者の保持する携帯電話の番号であり、前記利用者確認部は、利用者が保持する携帯電話を介して前記利用者への前記確認内容を音声情報により問い合わせ、利用者確認を得ることを特徴とする請求項 6 に記載の電子商取引システム。

【請求項 8】 前記電子透かし付与部が利用者の保持する携帯端末との通信手段を備え、前記利用者の連絡先データが利用者の保持する携帯端末のアドレス情報であり、前記利用者確認部は、前記携帯端末を介して前記利用者への前記確認内容を電子データとして問い合わせ、利用者確認を得ることを特徴とする請求項 6 に記載の電子商取引システム。

【請求項 9】 前記商取引情報に基づいて、手書きサインによるサイン認証処理を省略するか否かを判定する手書きサイン省略可否判定部を備え、

前記手書きサイン省略可否判定部により手書きサインの省略が認められた場合、前記手書きサイン入力部による電子サインデータ読み取りと、前記電子透かし付与部による電子透かし付き電子サインデータの生成が省略され、前記商取引データ格納部に前記読み取った利用者識別情報と前記商取引情報を格納する請求項 1 ～ 3 のいずれかに記載の電子商取引システム。

【請求項 1 0】 利用者と業者の間の商取引の正当性を検証する電子商取引システムであって、

前記商取引の内容を表わす商取引情報を受け取る商取引情報取得部と、

商取引に用いられた電子サインデータに対して該商取引を一意に特定する商取引識別子が電子透かし情報として付与された電子透かし付き電子サインデータを受け取る電子透かし付き電子サインデータ取得部と、

前記電子透かし付き電子サインデータの電子透かし情報を調べ、電子透かし付

き電子サインデータ改ざんされているか否かをチェックする改ざんチェック部と

前記電子透かし付き電子サインデータの電子透かし情報から商取引識別子を抽出する商取引識別子抽出部と、

前記商取引識別子により一意に特定される商取引情報を、事前に真正な商取引情報が格納されている商取引情報格納部の中から取得する商取引情報検索部と、

前記商取引情報取得部と前記商取引情報検索部でそれぞれ得られた商取引情報を比較・照合する検証部とを備えた電子商取引システム。

【請求項 1 1】 利用者と業者の間の商取引を扱う電子商取引方法であって、  
業者端末において利用者が提示した利用者識別情報を読み取り、  
前記業者端末において前記商取引の内容を表わす商取引情報を提示し、  
前記業者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子データとして読み取り、

第 3 者機関において前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と電子サインデータを取得し、

前記第 3 者機関において前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成し、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納することを特徴とした電子商取引方法。

【請求項 1 2】 利用者と業者の間の商取引を扱う電子商取引方法であって、  
業者端末において利用者が提示した利用者識別情報を読み取り、  
前記業者端末において前記商取引の内容を表わす商取引情報を提示し、  
前記利用者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子データとして読み取り、

第 3 者機関において前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と前記利用者端末からの電子サインデータとを取得し、

前記第 3 者機関において前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデ

ータを生成し、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納することを特徴とした電子商取引方法。

【請求項 1 3】 利用者と業者の間の商取引を扱う電子商取引方法であって、業者端末において利用者が提示した利用者識別情報を読み取り、

前記利用者端末が備える、前記業者端末から取得した前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

利用者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取り、

前記利用者端末において、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成し、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納することを特徴とした電子商取引方法。

【請求項 1 4】 前記第 3 者機関において前記利用者識別情報を基に予め登録されている前記利用者の真正サインデータを検索し、該真正サインデータを用いて前記電子サインデータの照合・認証を行うことを特徴とする請求項 1 1 ～ 1 3 のいずれかに記載の電子商取引システム。

【請求項 1 5】 利用者と業者の間の商取引の正当性を検証する電子商取引方法であって、

前記商取引の内容を表わす商取引情報を受け取り、

商取引に用いられた電子サインデータに対して該商取引を一意に特定する商取引識別子が電子透かし情報として付与された電子透かし付き電子サインデータを受け取り、

前記電子透かし付き電子サインデータの電子透かし情報を調べ、電子透かし付き電子サインデータ改ざんされているか否かをチェックし、

前記電子透かし付き電子サインデータの電子透かし情報から商取引識別子を抽出し、

前記商取引識別子により一意に特定される商取引情報を、事前に格納されてい



る真正な商取引情報の中から検索し、

前記受け取った商取引情報と前記検索した商取引情報を比較・照合して検証することを特徴とする電子商取引方法。

【請求項 1 6】 利用者と業者の間の商取引を扱う電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体であって、

業者端末において利用者が提示した利用者識別情報を読み取る処理ステップと

、  
前記業者端末において前記商取引の内容を表わす商取引情報を提示する処理ステップと、

前記業者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子データとして読み取る処理ステップと、

第 3 者機関において前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と電子サインデータを取得する処理ステップと、

前記第 3 者機関において前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する処理ステップと、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する処理ステップとを備えた処理プログラムを記録したことを特徴とする記録媒体。

【請求項 1 7】 利用者と業者の間の商取引を扱う電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体であって、

業者端末において利用者が提示した利用者識別情報を読み取る処理ステップと

、  
前記業者端末において前記商取引の内容を表わす商取引情報を提示する処理ステップと、

利用者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る処理ステップと、

第 3 者機関において前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と前記利用者端末からの電子サインデータとを取得する処理ステップと

前記第 3 者機関において前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する処理ステップと、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する処理ステップとを備えた処理プログラムを記録したことを特徴とする記録媒体。

【請求項 1 8】 利用者と業者の間の商取引を扱う電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体であって、

業者端末において利用者が提示した利用者識別情報を読み取る処理ステップと

前記利用者端末が備える、前記業者端末から取得した前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

利用者端末において提示された前記商取引情報に同意した利用者が入力する書きサインを電子サインデータとして読み取る処理ステップと、

前記利用者端末において、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する処理ステップと、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する処理ステップとを備えた処理プログラムを記録したことを特徴とする記録媒体。

【請求項 1 9】 前記処理プログラムが、前記第 3 者機関において前記利用者識別情報を基に予め登録されている前記利用者の真正サインデータを検索し、該真正サインデータを用いて前記電子サインデータの照合・認証を行う処理ステップを備えた処理プログラムである請求項 1 6 ～ 1 8 のいずれかに記載のコンピュータ読み取り可能な記録媒体。

【請求項 2 0】 利用者と業者の間の商取引を扱う電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体であって、

商取引に用いられた電子サインデータに対して該商取引を一意に特定する商取

引識別子が電子透かし情報として付与された電子透かし付き電子サインデータを受け取る処理ステップと、

前記電子透かし付き電子サインデータの電子透かし情報を調べ、電子透かし付き電子サインデータ改ざんされているか否かをチェックする処理ステップと、

前記電子透かし付き電子サインデータの電子透かし情報から商取引識別子を抽出する処理ステップと、

前記商取引識別子により一意に特定される商取引情報を、事前に格納されている真正な商取引情報の中から検索する処理ステップと、

前記受け取った商取引情報と前記検索した商取引情報を比較・照合して検証する処理ステップを備えた処理プログラムを記録したことを特徴とする記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、クレジットカードやデビットカードなど利用者識別情報が記録された媒体を使用して、利用者が業者との間で商取引を電子データのやり取りにより行う、いわゆる電子商取引を行う電子商取引システムおよび方法に関する。特に、手書きサインを電子データとして利用し、該電子サインに電子的な透かしを埋め込むことにより、利用者側、業者側、双方の不正を防止・抑止する電子商取引システムおよび方法に関する。

##### 【0002】

#### 【従来の技術】

クレジットカードを利用した商取引は、現在広く社会に普及しており、最近では利用者の銀行口座との間で即時に決済が行われるデビットカードも市場に導入され、ますます身近なものになってきている。このようなカードなど利用者識別情報を記録した媒体を用いる電子商取引では、真正の利用者であることを確認するために取引時に取引伝票に対して利用者のサインを筆記してもらい、これを業者側がカード背面の記入済の認証用の本人サインと比べることにより利用者が真正であることを確認し、利用者側のカードの不正利用を抑止するという方式が広く使われている。しかし、この方式では不正に他人のカードを入手した人が裏書

きのサインを練習して真似て筆記した場合には、特別に偽サインを見分ける訓練を受けていない人が偽サインであることを見破ることは難しいケースもあり、本人になり済ました偽サインによる不正使用を完全に防止することは難しい。また、利用者側からの万一のクレーム、取引内容の確認要求、取引監査に備えて、業者側は取引記録を残す必要があり、利用者がサインした紙の取引伝票を一定期間保管しているが、その保管に要する手間やコスト、取引伝票を検索する場合のコストも膨大である。

#### 【 0 0 0 3 】

このようなカードの不正使用を抑止する技術として、あるいは、取引伝票の保管のコストを削減する技術として、筆跡照合技術を利用し、タブレットなどのペン入力装置を利用して入力された電子サインと、あらかじめ登録されている利用者の電子サインを照合して、利用者の本人認証を行い、カードの不正使用を抑止するシステムが提案されている。例えば、公開番号特開平 1 0 - 3 2 0 4 6 5（カード与信・決済システム）には、業者端末が電子サインを入力する入力ポートを備えることによって、紙の取引伝票を不要にしてコストを削減する発明が開示されている。また、公開番号特開平 1 1 - 1 4 4 0 5 6（電子署名照合方式およびシステム）には、電子的に入力された手書き署名（サイン）と登録済のサインデータを照合し、本人であるか否かを判定する技術が開示されている。電子サインを用いて本人認証を行う技術では、利用者の書き順や筆圧、筆記速度など、最終的な筆跡形状からは読み取れない情報を利用して認証を行うことができるので、不正利用者が筆跡をまねて練習しても、これらの非形状情報を含めて一致しない限り偽サインであると判定することができるので、不正防止効果が高いと言える。

#### 【 0 0 0 4 】

これら従来の電子商取引方法を組み合わせたシステム構築例を図 1 1 を参照しつつ説明する。

#### 【 0 0 0 5 】

図 1 1 において、5 1 0 は業者側の店舗などに設置してある業者端末、5 2 0 が利用者識別情報が記録された記録媒体であるカードを読み取るカード読み取り

装置、530が利用者が手書きサインを入力する電子タブレットなどの電子サイン読み取り装置、540が業者端末の制御部、550が業者側のサーバの記憶部に設けられた取引情報を格納するための商取引情報格納部、560が手書きサインを基に利用者認証を行う認証センタが備える認証サーバ、570が認証サーバ560が備える利用者が真正サインとして登録した手書きサインを格納する登録サイン格納部、580が今回の商取引で入力された電子サインと登録サイン格納部570に格納された登録サインとの照合を行うサイン照合部、590が業者端末510と認証サーバ560の通信回線である。

#### 【0006】

商品などの購入の代金決済にあたり、利用者はカード読み取り装置520にクレジットカードなどを挿入して利用者識別情報を入力する。さらに利用者は電子サイン読み取り装置530を介して手書きサインを書き込み、電子サインとして入力する。業者端末510の制御部540は取得した利用者識別情報と電子サインを認証サーバ560に通信回線590を介して送信し、認証サーバ560はサイン照合部580において、入力された電子サインと登録サイン格納部570に格納された登録サインとの照合を行い、両者が一致すると判断した場合は、業者端末510の制御部540に対して利用者が真正のカード所有者であるとの利用者認証結果を報告する。業者端末510は商取引終了後、商取引に関する情報を業者側サーバ内の商取引情報格納部550に格納する。もし、サイン照合部580において電子サインが不正であることが疑わしい場合には制御部540に対して利用者認証ができなかった旨を報告する。業者端末510は当該取引を拒否したり、警告を発したり、または利用者にサインの再入力を促すなどの処理を行うことができる。上記の構成によれば、カードの不正利用を抑止することができ、また、取引情報を従来の紙媒体の取引伝票に代え、電子サインとともに業者側端末の記憶手段に電子データとして記憶することができ、紙伝票の保管コストや監査時の伝票検索コストなどを削減することができる。

#### 【0007】

##### 【発明が解決しようとする課題】

上記従来技術のように、カード取引時の手書きサインを電子化した電子サイン

とすれば、本人の登録サインと、商取引ごとに入力された電子サインとを、利用者の書き順や筆圧、筆記速度など、最終的な筆跡形状からは読み取れない情報を利用して認証を行うことができ、利用者側の不正使用を抑止する効果が高くなるほか、保存するデータが電子データであるので業者側の取引伝票保管に関するコストを大幅に低減することができる。

【 0 0 0 8 】

しかしながら、利用者側から見れば、自分の手書きサインが電子データとして業者側端末に取り込まれて保管されることとなり、業者側の悪意のサイン盗用、架空取引へのサイン複製、流用などの不正利用の可能性が大きくなりセキュリティ上の問題が発生する。つまり、利用者のサインが電子データとして業者端末に取り込まれるため、簡単に電子サインデータを盗用、複製することができ、業者側によって当該利用者の電子サインが悪用され、実際には行われていない架空取引に使われるなどの危険性を否定できない。

【 0 0 0 9 】

本発明の電子商取引システムおよび電子商取引方法は、取引伝票を電子化した商取引情報に対して電子的に入力された電子サインの単なる付加による利用者認証に代え、当該電子サインが、取引業者や第三者によって盗用、複製されることを防止し、架空取引などに悪用されることを効果的に防止した電子商取引システムおよび電子商取引方法を提供することを目的とする。

【 0 0 1 0 】

さらに、従来の紙媒体の取引伝票に対する手書きサインによる利用者認証に比べ、認証精度が高く、かつ、取引業者の取引情報の保存コスト、検索コストを低減する電子商取引システムおよび電子商取引方法を提供することを目的とする。

【 0 0 1 1 】

【課題を解決するための手段】

上記課題を解決するために、本発明の電子透かし付き電子サインを用いた電子商取引システムは、利用者と業者の間の商取引を扱う電子商取引システムであって、業者端末が備える、利用者が提示した利用者識別情報を読み取る利用者識別情報読み取り部と、前記業者端末が備える、前記商取引の内容を表わす商取引情

報を提示する商取引情報提示部と、前記業者端末が備える、提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る手書きサイン入力部と、第3者機関が備える、前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と電子サインデータを取得し、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する電子透かし付与部と、前記業者端末が備える、前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する商取引データ格納部とを備えたことを特徴とする。

## 【 0 0 1 2 】

上記構成により、商取引に関する情報の保存および管理が電子データの形で行うことができ、取引の利便性が高まり、データの保存コスト、監査時の検索コストの低減も可能となる。また、電子透かし付き電子サインを埋め込んだ電子透かし付き電子サインデータを生成するので、業者による電子サイン盗用防止および悪意の架空取引への流用が防止できる。また、電子透かし付与部が利用者および事業主体とは異なる第三者機関が管理・運用しているのでカード不正利用、業者側の手書きサイン盗用、架空取引への流用に対するセキュリティが向上する。

## 【 0 0 1 3 】

なお、上記構成では、手書きサイン入力部を業者端末に設ける構成としているが、該構成に代え、利用者端末に設ける構成とすることも可能である。

## 【 0 0 1 4 】

この構成によれば、手書きサイン入力部が利用者端末に設けられているので、業者端末に設けた構成よりもさらに業者による電子サイン盗用防止および悪意の架空取引への流用を防止するセキュリティが高まり、さらに、利用者が電子サインを入力することへの抵抗感が薄まるという心理的效果も期待できる。

## 【 0 0 1 5 】

なお、上記構成では、電子透かし付与部を第3者機関に設けた構成としているが、該構成に代え、利用者端末に設ける構成とすることも可能である。

## 【 0 0 1 6 】

この構成によれば、電子透かし付与部が利用者端末に設けられているので、電

子透かし付与処理に対する利用者確認を不要とすることができる。

【 0 0 1 7 】

また、第 3 者機関が、前記利用者識別情報を基に予め登録されている前記利用者の真正サインデータを検索し、該真正サインデータを用いて前記電子サインデータの照合・認証を行うサイン認証部を備えることが好ましい。

【 0 0 1 8 】

上記構成により、商取引の際に、電子サインデータと真正サインデータを用いた利用者の認証を実行することができ、商取引のセキュリティがさらに向上する。

【 0 0 1 9 】

次に、本発明の電子商取引システムにおいて、前記電子透かし付与部が、認証された電子サインデータを予め指定されたビット長の電子データに要約した要約情報を生成する電子サインデータ要約部を備え、前記商取引識別子に加えて前記要約情報も電子透かし情報として前記電子サインデータに対して付与することが好ましい。

【 0 0 2 0 】

上記構成により、電子透かし情報として前記商取引識別子に加え、電子サインデータから一意に生成される要約情報を付与することができるため、電子サインの偽造に対するセキュリティがさらに向上することとなる。

【 0 0 2 1 】

また、本発明の電子商取引システムにおいて、前記電子透かし付与部が、前記業者端末を介した電子サインデータの送信があった場合に、登録されている利用者の連絡先データを基に利用者に対して直接、該商取引における電子透かし付き電子サインデータ生成是非の確認を行う利用者確認部を備え、前記利用者確認部は、前記利用者からの確認が得られない場合には前記業者端末に対して前記電子透かし付き電子サインデータの生成の拒否を通知することとすれば、商取引の成立の前に、第三者が介在しない形で事前に利用者に対して利用者確認を得ることができ、利用者からの確認が得られない場合には、電子透かし付き電子サインデータの生成の拒否を通知することができ、セキュリティを高く維持することがで



きる。

【 0 0 2 2 】

また、上記電子商取引システムにおいて、前記商取引情報に基づいて、手書きサインによる認証処理を省略するか否かを判定する手書きサイン省略可否判定部を備え、前記手書きサイン省略可否判定部により手書きサインの省略が認められた場合、前記手書きサイン入力部による電子サインデータ読み取りと、前記電子透かし付与部による電子透かし付き電子サインデータの生成が省略され、前記商取引データ格納部に前記読み取った利用者識別情報と前記商取引情報を格納することも可能である。

【 0 0 2 3 】

この構成によれば、商取引のセキュリティレベルが低くなるが、商取引の金額・種別などによっては商取引処理手続を簡略化しても実運用上に耐え得ると扱える場合では問題とはならず、商取引の処理内容を低減することができるので処理の効率化を図ることができる。

【 0 0 2 4 】

次に、本発明は、商取引完了後に決済機関側や業者側で過去の該商取引情報の真正性が問題となった場合などに商取引内容の検証を行うシステムも提供する。利用者と業者の間の商取引の正当性を検証する電子商取引システムであって、前記商取引の内容を表わす商取引情報を受け取る商取引情報取得部と、商取引に用いられた電子サインデータに対して該商取引を一意に特定する商取引識別子が電子透かし情報として付与された電子透かし付き電子サインデータを受け取る電子透かし付き電子サインデータ取得部と、前記電子透かし付き電子サインデータの電子透かし情報を調べ、電子透かし付き電子サインデータ改ざんされているか否かをチェックする改ざんチェック部と、前記電子透かし付き電子サインデータの電子透かし情報から商取引識別子を抽出する商取引識別子抽出部と、前記商取引識別子により一意に特定される商取引情報を、事前に真正な商取引情報が格納されている商取引情報格納部の中から取得する商取引情報検索部と、前記商取引情報取得部と前記商取引情報検索部でそれぞれ得られた商取引情報を比較・照合する検証部とを備えたことを特徴とする。

## 【 0 0 2 5 】

上記構成により、入力された検証が求められている商取引情報と、別途格納されている真正の商取引情報の中から電子透かし付き電子サインデータを基に一意に特定された真正の商取引情報とを比較し、当該検証が求められている商取引情報が真正であるか否かを検証することができる。

## 【 0 0 2 6 】

本発明の電子透かし付き電子サインを用いた電子商取引システムは、上記の電子透かし付き電子サインを用いた電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体から処理プログラムを読み込むことにより、コンピュータを用いて構築することができる。

## 【 0 0 2 7 】

## 【発明の実施の形態】

本発明の電子商取引システムおよび電子商取引方法の実施形態を以下に示す。以下では、典型例として店頭でのクレジットによる商品購入の商取引に適用した例を説明するが、本発明はサインが本人認証に用いられるアプリケーションに対して適用可能である。

## 【 0 0 2 8 】

## (実施形態 1)

実施形態 1 の電子商取引システムおよび電子商取引方法を図を参照しつつ説明する。

## 【 0 0 2 9 】

図 1 は、実施形態 1 の電子商取引システムの構成例を示すブロック図である。

## 【 0 0 3 0 】

図 1 において、10 は業者端末、20 は利用者識別情報読み取り部、30 は手書きサイン入力部、40 は業者端末の制御部、50 が商取引データ格納部、60 がデータ送受信部である。本実施形態 1 の構成では、業者端末 10 が手書きサイン入力部 30 を持った構成であり、当該手書きサイン入力部 30 が商取引情報提示部 31 を備えている。

## 【 0 0 3 1 】

1 0 0 は第三者機関である電子サイン管理機関が管理する電子サイン管理サーバである。電子サイン管理サーバ 1 0 0 は、データ送受信部 1 1 0、電子透かし付与部 1 5 0、商取引管理データ格納部 1 6 0 を備えている。なお、本実施形態 1 では、業者端末 1 0 が取引内容入力部 1 1 を備え、電子透かし付与部 1 5 0 が、電子透かし情報取得部 1 5 1、電子サインデータ要約処理部 1 5 2、電子透かし付与処理部 1 5 3、利用者確認部 1 5 4 を備えた構成となっている。

#### 【 0 0 3 2 】

2 0 0 は決済機関のサーバである。決済機関のサーバ 2 0 0 は、商取引情報生成部 2 1 0 を備えている。ここで、決済機関と電子サイン管理機関は、利用者や業者とは異なる第三者機関とする。なお、決済機関と電子サイン管理機関は、別機関であっても良く、同じ機関が兼ねるものでも良い。ただし、また、商取引情報生成部 2 1 0 は電子サイン管理サーバ 1 0 0 内に備える構成としても良い。

#### 【 0 0 3 3 】

3 0 0 はネットワークであり、電話回線やインターネットなどである。4 0 0 は利用者が携帯している携帯電話などの携帯端末である。

#### 【 0 0 3 4 】

図 1 に示した構成要素を簡単に説明する。

#### 【 0 0 3 5 】

業者端末 1 0 は、業者の店舗内に設置された端末で電話回線やインターネットなどにより決済機関のサーバ 2 0 0 や電子サイン管理機関の電子サイン管理サーバ 1 0 0 と接続されている。

#### 【 0 0 3 6 】

取引内容入力部 1 1 は、業者が商取引に際して、商品の代金、商品コードなど取引内容に関する情報を業者端末 1 0 に入力する部分であり、例えば、業者店舗に設置されているレジスタや P O S 端末から入力された商品の代金、商品コードなど取引内容に関する情報を業者端末 1 0 に送信する構成でも良い。

#### 【 0 0 3 7 】

利用者識別情報読み取り部 2 0 は、利用者識別情報を読み取る部分で、利用者識別情報を記録した記録媒体に応じて様々な形態がある。例えば、磁気ストライ

ブ付きカードであれば、カードの磁気ストライプリーダとなり、ＩＣカードであれば、ＩＣカードリーダとなり、また、暗証番号（ＰＩＮ番号）が併用される場合にはＰＩＮ番号入力テンキーが備えられる。指紋や声紋などバイオメトリック情報を利用する場合は、それら情報を読み取る専用デバイスが搭載される。

## 【 0 0 3 8 】

手書きサイン入力部 3 0 は、手書きサインを電子データとして読み取る部分であり、例えば、電子タブレットなどである。電子データ化できるものであれば、電磁誘導式タブレット、感圧式タブレット、光学式タブレットなど種類の如何を問わないが、最終的な筆跡形状のみならず、利用者の書き順、筆圧、筆記速度など手書きサインに関して照合に用いる多様な情報を読み取れることが好ましい。

## 【 0 0 3 9 】

商取引情報提示部 3 1 は、利用者がサインするにあたり、商取引内容である商取引情報を確認するために該情報を利用者に提示する部分である。ここで、商取引情報とは、業者番号、業者伝票番号、取引金額などを含む商取引内容を表わす情報であり、特に、取引金額は業者による改ざんを防止する目的から商取引情報に必須の情報とする。本実施形態 1 の構成では商取引情報は決済機関のサーバ 2 0 0 が備える商取引情報生成部 2 1 0 により生成される。生成に際しては業者端末 1 0 において取引内容入力部 1 1 を介して入力された取引内容を示す情報、利用者識別情報読み取り部 2 0 を介して読み取られた利用者識別情報が決済機関のサーバ 2 0 0 に送信され、決済機関のサーバ 2 0 0 においてそれら情報を基に商取引情報が生成される。従来の紙伝票処理におけるサインが空欄状態の伝票にあたる。利用者は商取引情報提示部 3 1 が提示した商取引情報の内容を確認して同意すれば手書きサイン入力部 3 0 を介して手書きサインを入力する。ここで、商取引情報提示部 3 1 が手書きサイン入力部 3 0 の電子タブレットなどを利用して商取引情報を提示する構成とすれば、電子タブレット上に提示された商取引情報のサイン欄に手書きサインを入力するという運用が可能となる。

## 【 0 0 4 0 】

業者端末の制御部 4 0 は、業者端末 1 0 の動作を制御する部分である。

## 【 0 0 4 1 】

商取引データ格納部 5 0 は、商取引が成立し、完了した後、電子透かし付き電子サインデータを格納・保存する部分である。

【 0 0 4 2 】

データ送受信部 6 0 は、電子サイン管理サーバ 1 0 0 や決済機関のサーバ 2 0 0 との間でデータの送受信を行う部分で、通信インタフェースを備えている。

【 0 0 4 3 】

次に、決済機関のサーバ 2 0 0 を説明する。決済機関のサーバ 2 0 0 は、クレジット会社や銀行などの決済機関が管理するサーバであり、決済に関する信用保証を行う処理を行う。決済機関のサーバ 2 0 0 は商取引情報生成部 2 1 0 を備えている。業者端末 1 0 から送信された取引内容を示す情報と利用者識別情報を基に商取引情報が生成される。信用保証は商取引情報に真正と判定された電子透かし付き電子サインデータが埋め込まれた商取引情報、つまり、電子透かし付き電子サインデータが得られた場合に与えられるものとする。

【 0 0 4 4 】

次に、電子サイン管理サーバ 1 0 0 の構成要素を簡単に説明する。

【 0 0 4 5 】

データ送受信部 1 1 0 は、業者端末 1 0 との間でデータの送受信を行う部分で、通信インタフェースを備えている。

【 0 0 4 6 】

なお、任意の構成として利用者認証部を備えても良い。利用者認証部は、今回の取引の利用者を真正な利用者であると認証する部分である。サイン照合部 1 3 0 から渡されるサインが真正であるか否かの情報に加え、必要に応じて他に入力された暗証番号やバイオメトリック情報、カードの紛失届に関する情報など、利用者の正当性を確認する情報を用いて利用者を認証する。もちろん処理を簡素化し、サインが真正であるか否かの情報のみで利用者が真正であると判断する処理とすることも可能である。

【 0 0 4 7 】

本実施形態 1 では必須構成として電子透かし付与部 1 5 0 を備えている。電子透かし付与部 1 5 0 は、業者端末 1 0 から得た商取引情報と手書きサイン入力部

30から入力された電子サインデータに対して、電子透かし情報を埋め込み、電子透かし付き電子サインデータを生成する部分である。

【0048】

なお、本実施形態1では任意の構成として商取引管理データ格納部160を備えている。商取引管理データ格納部160は、電子透かし付与部150により生成された電子透かし付き電子サインデータを登録保持しておく部分である。将来、商取引者間において何らかのトラブルが発生した場合に備えて生成した電子透かし付き電子サインデータを登録しておく。

【0049】

次に、電子透かし付与部150の各構成要素を説明する。

【0050】

電子透かし情報取得部151は、電子透かし情報とする情報を取得する部分である。電子透かし情報の一例としては、今回の取引内容を示す商取引識別子、利用者の電子サインデータから生成した要約情報がある。ここで、商取引識別子は、取引内容を個別に特定・識別しうる情報であり、例えば、シリアルに付される番号や暗号のようなものでも良い。さらに、商取引識別子は、少なくとも、該商取引に関わる業者を特定する業者識別情報、該商取引に関わる利用者を特定する利用者識別情報、該商取引を特定するため業者側が付与した商取引業者管理情報、該利用者が入力した電子サインデータ、該商取引に関わる決済金額情報、該商取引の発生した日時情報を含むものであるものでも良い。これら情報は、今回の取引内容を示す商取引を識別するには有効な情報であると考えられるからである。商取引識別子は、業者端末10から送信され、データ送受信部110を介して電子サイン管理サーバ100に受信される。

【0051】

本実施形態1では、付加情報として利用者の電子サインデータから生成した要約情報も用いる。要約情報は電子サインデータ要約処理部152により生成する。電子サインデータ要約処理部152はデータ長要約アルゴリズムに従って、電子サインデータを所定のデータ長となるように圧縮する部分である。電子署名データが改ざんされると、抽出された要約情報と、もう一度計算によって得られる

要約情報に違いが検出されるため、改ざんがあったことが検知できる。

【 0 0 5 2 】

電子透かし付与処理部 1 5 3 は、電子サインデータに対して電子透かし情報を埋め込む処理を実行する部分である。

【 0 0 5 3 】

以下に、電子透かし付与処理部 1 5 3 による電子透かし付与処理を詳しく説明する。電子透かしは、電子的なデータの不正コピーを防止することを目的とするもので、電子サインデータに「電子透かし」を埋め込むことにより様々な効果を得ることができる。例えば、人間には外見上「電子透かし」が埋め込まれているかを識別できない。また、電子透かしを埋め込んだ電子サイン管理機関側は必要に応じていつでも透かし情報を読み取ることができる。また、埋め込みアルゴリズムを知らない限り、第三者が電子データから透かし情報を取り除くことはできない。さらに、無理に透かし情報を取り除くと、改ざんがあったことが検知でき、不正なデータであることが判定できる。電子サインデータへの電子透かしの埋め込み方法は複数あり、電子サインデータのデータ形式に応じて使い分けることも可能である。電子サインデータは典型的には 2 値あるいは他値にビットマップ化された静止画イメージで表現されている場合と二次元の座標点の時系列データとして表現されている場合がある。本実施形態 1 では、サイン照合をより高精度に実行できる二次元の座標点の時系列データで表現されている場合の電子サインデータに対して電子透かし情報を埋め込む処理を例として説明する。

【 0 0 5 4 】

電子サインデータは、手書きサイン入力部 3 0 を介して取り込まれるが、手書きサイン入力部 3 0 として、電磁誘導式タブレット、感圧式タブレットなど、文字の筆記に伴うペン先の位置と状態の変化を一定時間間隔で検知するデバイスが使われる。このデバイスを使用した場合、図 2 ( a ) のような電子サインデータは、図 2 ( b ) のような、座標点の列のデータとして表現される。正確に言えば、座標点  $P_i$  の位置座標を  $X_i$ 、 $Y_i$ 、その時の属性値を  $S_i = (\text{PenDown}, \text{PenMove}, \text{PenUp})$  とし、座標点  $P_i$  は  $P_i : (X_i, Y_i, S_i)$  として表現される。そのとき、電子サインデータ全体は  $\text{Sign} = (n, P_1, P_2, \dots, P_n$

)( $n$ は自然数であり、座標点数により可変)として表現される。ここでPenDownとは、文字の一面(ストロークと呼ぶ)の第一点、PenUpはストロークの最終点、PenMoveはストロークの途中の点につけられる属性値である。タブレットによっては、属性値として、その時点の筆圧を量子化した情報、筆記開始からの経過間情報、ペンの傾き値情報などの持つ場合もあるし、電子誘導式のようにペンがある程度筆記面から離れていても座標値を検出できる場合には、PenUpがストロークの最終点だけでなく、ペン先が空中を移動している時間にサンプリングした座標点にも付与される場合もある。

## 【0055】

電子サインデータに電子透かし情報を埋め込む場合は、人間には検知できない電子データの冗長性部分を利用して行うことが好ましい。電子サインデータの場合、例えば、次のような手法が考えられる。

## 【0056】

第1の手法は、位置座標の下位ビットに情報を埋め込む手法である。座標点の位置座標( $X_i, Y_i$ )を、それぞれ16ビットで表現したとする。この場合、 $X$ 座標、 $Y$ 座標は縦、横それぞれ65536の解像度を持つことになる。文字をディスプレイ上に表現するには $100 \times 100$ ドット程度の解像度があれば十分であり、このような低解像度でも、 $X$ または $Y$ 座標値が $\pm 1$ 程度変化しても人間の目には殆ど感知できない。さらに解像度を上げて16ビット程度で表現してしまえば、下位1~2ビットを電子透かし情報の埋め込みに使っても人間の目に感知することはできず、サイン照合アルゴリズムも、この程度の変化で影響を受けることはない。このような性質を利用して $Sign = (n, P_1, P_2, \dots, P_n)$  ( $n$ は自然数であり、座標点数により可変)のうち、電子透かし埋め込みアルゴリズムが定める複数の点 $P_{j1}, P_{j2}, \dots, P_{jm}$ を選んで、 $XY$ 座標値の下位ビットに透かし情報を埋め込む。どの点に埋め込むかは、もちろん非公開であり、それ以外の点に錯乱のためにデータを混入してもよい。

## 【0057】

第2の手法は、冗長な座標点を埋め込む手法である。電子サインデータがディスプレイやプリンタに表示される時、PenDownからPenUpまでの一連の点列は折れ線



(またはより滑らかにするためスプライン曲線やベジエ曲線)で繋がれて、通常座標点自体が明確に表示されることはない。このため、PenMoveの段階で $P_i$ と全く同一の点が $P_i$ の後に挿入されて $Sign = (n+1, P_1, P_2, \dots, P_i, P_i, \dots, P_n)$  ( $n$ は可変)となっても、人間の目に知覚できない。このように同じ位置座標を持つ点を連続して埋め込むことによって透かし情報を埋め込むことが可能である。

## 【0058】

第3の手法は、冗長な座標点を埋め込む手法で上記第2の手法と異なるものである。第2の手法は、全く同じ座標点が連続することになるので、同じ座標点が連続しているか否かを探知することにより、どれが電子透かし情報の座標点であるか見破られやすい。そこで、まったく同じ座標値を埋め込むのではなく、図3のように連続する二つの座標点 $P_i, P_{i+1}$ の間に、 $P_i$ と $P_{i+1}$ を $N:M$ に内分する座標点 $P_i'$ を埋め込む。この場合、座標点 $P_i'$ が埋め込まれてもやはり人間に変化を感知することはできない。また、この場合は何対何に内分するかという自由度があり、これによって電子透かし情報の埋め込みにおいて複数の選択冗長が得られ、どの点が埋め込まれた座標点であるか容易には検知できないため安全性が高くなる。例えば、 $N:M$ が $1:1, 1:2, 1:3, 1:4$ のいずれかとすれば座標点の埋め込み1点あたり2ビット分の冗長性が得られ、4通りの埋め込みが可能となる。どの位置 $P_i$ に埋め込むかは、当然非公開とする。

## 【0059】

以上、電子サインデータへの電子透かし情報の埋め込み手法を説明したが、本発明の電子商取引システムおよび方法において、上記埋め込み手法以外にも用いることができ、また、同時に複数の手法を組み合わせることでより埋め込み情報量を増やしたり、安全性を高めることも可能である。

## 【0060】

埋め込みアルゴリズムを秘密にすれば、第三者に埋め込んだ情報を読み取られる危険性は少ないが、これだけでは電子サインデータの改ざんを防止できない。そのため本発明の電子商取引システムおよび方法では改ざん防止手法として、電

子サインデータ要約処理部 1 5 2 により電子サインデータ全体に対して要約関数を適用し、所定ビットの要約情報を生成する。要約情報のビット量としては、8 ビット程度でも実用上十分である。この要約情報を付加情報として電子透かし情報取得部 1 5 1 に渡し、電子透かしデータの一部として用い、N ビットの要約情報を電子透かしとして埋め込む。電子署名データが改ざんされると、抽出された要約情報と、もう一度計算によって得られる要約情報に違いが検出されるため、改ざんがあったことが検知できる。

#### 【 0 0 6 1 】

電子透かし付与部 1 5 0 は、上記のように電子サインデータに対して電子透かし情報を埋め込み、電子透かし付き電子サインデータを生成する。さらに、商取引における何らかのトラブルに備えるべく、電子透かし付き電子サインを商取引管理データ格納部 1 6 0 に登録保持しておくことが好ましい。

#### 【 0 0 6 2 】

本実施形態 1 の構成は利用者確認部 1 5 4 を備えている。利用者確認部 1 5 4 は、登録されている利用者の連絡先データを基に利用者に対して直接、該商取引における電子透かし付き電子サインデータ生成の是非の確認を行う部分である。業者側の偽サインの流用による架空の取引を防止するためのセキュリティ向上手段の一つである。取引を成立させる前に利用者に対して確認をとるもので、業者端末 1 0 を介さずに、利用者確認部 1 5 4 と利用者がネットワーク 3 0 0 などの通信路を介して直接通信し合うことが好ましい。

#### 【 0 0 6 3 】

例えば、利用者の連絡先データとして携帯電話の番号を保持し、利用者の携帯電話を利用して利用者確認部 1 5 4 と利用者が電話回線を介して確認内容の問い合わせをする。この場合、利用者確認部 1 5 4 が電話通信手段と音声応答システムを備え、利用者の携帯電話などの携帯端末 4 0 0 を介して利用者への確認内容を音声情報により問い合わせ、利用者確認を得ることも可能である。一例として、コンピュータの音声合成により「取引を承認する場合は「1」のボタン、承認しない場合は「0」のボタンを押して下さい」とのメッセージを発生し、「登録判定プログラム」は利用者のボタン操作によって登録確認の可否を判断する。ま

た、他の例としては、利用者確認部 1 5 4 が、利用者が保持する携帯端末 4 0 0 との通信手段を備え、携帯端末 4 0 0 を介して利用者への確認内容を電子データとして問い合わせ、電子データにより確認を得る。利用者端末がマルチメディア電子メール等を受信できる装置であれば、「利用者認証機関」は例えばジャバスクリプトにより記述された返信応答ボタンが付与された HTML 表現の電子メールを利用者端末に送付し、画面上に「〇〇の取引を承認する場合には、「YES」ボタン、承認しない場合は「NO」ボタンを押して下さい」という案内で確認操作の指示をすることもできる。また、音声認識部を備え、音声で「はい」とか「いいえ」で答えるようにしても良い。

## 【 0 0 6 4 】

利用者確認部 1 5 4 は、利用者からの確認が得られない場合は、電子透かし付き電子サインデータの生成を拒否することとし、業者端末の制御部 4 0 に対して拒否の旨を通知する。

## 【 0 0 6 5 】

このように業者端末 1 0 を介さずに利用者確認部 1 5 4 と利用者が直接通信し合うことで架空の取引を取引成立前に事前に察知することができ、電子商取引システムのセキュリティを向上することが可能となる。

## 【 0 0 6 6 】

次に、本実施形態 1 の電子商取引システムおよび方法の動作の流れを図 4 のフローチャートを参照しつつ説明する。

## 【 0 0 6 7 】

まず、利用者と業者の間で商品購入など取引内容が定められる。業者は、業者コード、業者が個々の取引を識別するために付与する取引コード、取引金額など取引内容に関する情報を取引内容入力部 1 1 を介して業者端末 1 0 に入力し、一方、利用者は利用者識別情報を利用者識別情報読み取り部 2 0 を介して業者端末 1 0 に入力する（ステップ S 4 0 1）。なお、カード媒体から利用者識別情報を読み取る場合は、業者が利用者に代わってカードを利用者識別情報読み取り部 2 0 であるカードリーダーに挿入して読み取られせることも可能である。バイオメトリック情報である場合などは利用者自らが利用者識別情報読み取り部 2 0 を操作

する。

【 0 0 6 8 】

業者端末の制御部 4 0 は、取引内容に関する情報と利用者識別情報を決済機関のサーバ 2 0 0 に送る。決済機関のサーバ 2 0 0 はカードの有効性や利用者に対する信用枠、業者が加盟業者であるかなどを確認し、商取引情報生成部 2 1 0 により商取引情報を生成する（ステップ S 4 0 2）。なお、決済機関のサーバ 2 0 0 と業者端末 1 0 とは専用回線あるいはインターネット、無線通信回線などの電子データを相互に送受信できるネットワーク 3 0 0 にて結ばれているものとする。

【 0 0 6 9 】

生成された商取引情報は決済機関のサーバ 2 0 0 から商取引情報提示部 3 1 に渡され、商取引情報提示部 3 1 は商取引情報を利用者に提示する（ステップ S 4 0 3）。

【 0 0 7 0 】

利用者は、提示された商取引情報から取引内容を確認し（ステップ S 4 0 4）、取引に同意する場合（ステップ S 4 0 4 : Y）、手書きサイン入力部 3 0 を介して手書きサイン欄にサインを手書き入力する（ステップ S 4 0 5）。

【 0 0 7 1 】

手書きサイン入力部 3 0 は、手書き入力されたサインから、最終的な筆跡形状、書き順、筆圧、筆記速度など照合処理に用いる情報を電子化した電子サインデータを得て、電子サインデータと商取引情報を電子サイン管理サーバ 1 0 0 に送信する（ステップ S 4 0 6）。なお、電子サイン管理サーバ 1 0 0 と業者端末 1 0 とは専用回線あるいはインターネット、無線通信回線などの電子データを相互に送受信できるネットワーク 3 0 0 にて結ばれているものとする。

【 0 0 7 2 】

次に、電子サイン管理サーバ 1 0 0 は、データ送受信部 1 1 0 を介して電子サインデータと商取引情報を受け取る。なお、ここで、他の暗証番号やバイオメトリック情報、カードの紛失届に関する情報など、利用者の正当性を確認する情報がある場合には当該情報を用いて利用者をチェックすることもできる。

## 【 0 0 7 3 】

本実施形態 1 の構成では、利用者確認部 1 5 4 により、利用者に対して直接、電子透かし付き電子サインデータ生成を実行しても良いか確認する（ステップ S 4 0 7）。つまり、利用者の保持する携帯電話や携帯端末を介して音声案内や電子データにより本人に対して該商取引における電子透かし付き電子サインデータ生成の是非の確認を行う。

## 【 0 0 7 4 】

利用者からの確認が得られれば（ステップ S 4 0 7 : Y）、電子透かし付与部 1 5 0 による処理が開始する。本実施形態 1 の構成では、電子サインデータ要約処理部 1 5 2 により電子サインデータから要約情報を生成し（ステップ S 4 0 8）、電子透かし情報取得部 1 5 1 が今回の取引内容を特定する商取引識別子や要約情報などを電子透かし情報として取得し（ステップ S 4 0 9）、電子透かし付与処理部 1 5 3 が非公開のアルゴリズムにより電子サインデータに対して電子透かしとして埋め込み、電子透かし付き電子サインデータを生成する（ステップ S 4 1 0）。

## 【 0 0 7 5 】

なお、電子サイン管理サーバ 1 0 0 は、商取引における何らかのトラブルに備えるべく、電子透かし付き電子サインを商取引管理データ格納部 1 6 0 に登録する。さらに、電子サイン管理サーバ 1 0 0 はデータ送受信部 1 1 0 を介して、生成した電子透かし付き電子サインデータを業者端末 1 0 に送信し、商取引データ格納部 5 0 に格納する（ステップ S 4 1 1）。

## 【 0 0 7 6 】

なお、この電子透かし付き電子サインデータは、業者端末 1 0 からまたは電子サイン管理サーバ 1 0 0 から決済機関のサーバ 2 0 0 に対して送信され、決済機関により該商取引に対する信用保証が与えられる。

## 【 0 0 7 7 】

なお、上記ステップ S 4 0 4 において取引に同意しない場合（ステップ S 4 0 4 : N）、上記ステップ S 4 0 7 において利用者からの確認が得られなかった場合（ステップ S 4 0 7 : N）は、いずれも、今回の商取引に対する信用保証を与

えることができないとして、電子商取引処理を終了する。

【 0 0 7 8 】

以上が、本実施形態 1 の電子商取引システムおよび方法の処理の流れである。もちろん、上記処理の流れは一例であり、本発明の技術思想の及ぶ範囲において他の処理の流れとすることも可能である。

【 0 0 7 9 】

なお、決済機関における処理として、商取引情報を電子透かしとして電子透かし付き電子サインデータを生成し、該情報を決済機関側でも格納しておき、決済時に決済機関側において、業者端末側が送ってきた電子透かし付き電子サインデータと照合するという決済手順も可能である。

【 0 0 8 0 】

上記構成による電子商取引システムおよび方法とすることにより、業者は電子透かし付き手書き電子署名データを複製したり、他の架空取引に流用するような行為を行うことはできない。実際にそのような行為が行われれば、架空取引に関する電子透かし付き電子サインデータを基に、電子サイン管理機関に対して、商取引管理データ格納部 1 6 0 に登録された電子透かし付き電子サインを検索し、正式に商取引として登録されたものであるか、正式に登録されたものであれば、いつ、なんの取引の時に使用した電子サインであるかを知ることができるからである。

【 0 0 8 1 】

また、応用的な運用として、電子サイン管理機関は、利用者認証時に利用者に直接確認を行うことにより、業者、あるいは、第三者によって、利用者が認知しない架空のサイン登録が電子サイン管理機関に行われることを防ぐことができる。この応用的な運用を行う場合、利用者が携帯端末を該商取引実行時に保持している必要があるが、近年の携帯電話や i モードの普及率を見れば、このような運用も十分期待できる。また、当該確認は、取引時にリアルタイムに実施しなくても、例えば、一日以内、あるいは一週間以内に行い、その段階で利用者承認が得られなければ商取引の取り消し（無効）を実施するというものでも良い。この場合には、利用者確認部は、有線電話通信、F A X 通信、電子メール通信、手紙

等任意の手段であっても良い。

【 0 0 8 2 】

(実施形態 2)

実施形態 2 の電子商取引システムおよび電子商取引方法を図を参照しつつ説明する。

【 0 0 8 3 】

図 5 は、実施形態 2 の電子商取引システムの構成例を示すブロック図である。

【 0 0 8 4 】

図 5 において、電子サイン管理サーバ 1 0 0 a、決済機関のサーバ 2 0 0 a、ネットワーク 3 0 0 の諸構成要素は実施形態 1 で説明した図 1 と同様であるが、業者端末 1 0 a は利用者識別情報読み取り部 2 0、業者端末の制御部 4 0、商取引データ格納部 5 0、データ送受信部 6 0 を備えているが、手書きサイン入力部 3 0 および商取引情報提示部 3 1 が設けられておらず、利用者の携帯端末 4 0 0 a が手書きサイン入力部 3 0 および商取引情報提示部 3 1 を備えた構成となっている。なお、各要素は実施形態 1 と同様であるのでここでの説明は省略する。

【 0 0 8 5 】

図 5 の構成によれば、手書きサイン入力部 3 0 が業者端末 1 0 に接続されていないので、利用者が保持する携帯端末 4 0 0 a を介して利用者と電子サイン管理サーバ 1 0 0 a が直接データ通信し合うことにより電子サインデータがやりとりでき、悪意の業者によるサインの盗用や複製といった不正行為に対するセキュリティ強度がさらに向上する。

【 0 0 8 6 】

図 5 の構成の場合、決済機関のサーバ 2 0 0 a の商取引情報生成部 2 1 0 が生成した商取引情報が直接、利用者の携帯端末 4 0 0 a に送信され、商取引情報提示部 3 1 に提示されることとなる。利用者は商取引情報の内容を確認し、手書きサイン入力部 3 0 に対して手書きサインを書き込む。利用者の携帯端末 4 0 0 a は、商取引情報と電子サインデータを電子サイン管理サーバ 1 0 0 a に対して直接送信する。電子サイン管理サーバ 1 0 0 a において電子透かしが付され、業者端末 1 0 に対しては、電子透かし付き電子サインデータという形で渡されること

となり、実施形態 1 のように、電子透かしが未だ付されていない状態の電子サインデータが業者端末 1 0 a を経由することはない。それゆえ、悪意の業者によるサインの盗用や複製といった不正行為に対するセキュリティがさらに向上する。さらに、利用者は業者端末 1 0 a に接続された手書きサイン入力部 3 0 に対して入力する必要がないので、プライバシー保護が向上し、心理的效果として安心して電子商取引を行うことができる。

#### 【 0 0 8 7 】

本実施形態 2 の電子商取引システムおよび方法の動作の流れを図 6 のフローチャートを参照しつつ説明する。

#### 【 0 0 8 8 】

まず、取引内容入力部 1 1 および利用者識別情報読み取り部 2 0 を介した取引内容に関する情報および利用者識別情報の入力処理（ステップ S 6 0 1）、決済機関のサーバ 2 0 0 a の商取引情報生成部 2 1 0 による商取引情報の生成（ステップ S 6 0 2）は実施形態 1 に示した図 4 のフローチャートに示したステップ S 4 0 1 とステップ S 4 0 2 の処理と同様である。

#### 【 0 0 8 9 】

次に、決済機関のサーバ 2 0 0 a は、生成した商取引情報を、無線電話回線などのネットワーク 3 0 0 を通じて、利用者が保持する携帯電話などの携帯端末 4 0 0 a に対して直接送信し、携帯端末 4 0 0 a の商取引情報提示部 3 1 は受信した商取引情報を利用者に提示する（ステップ S 6 0 3）。

#### 【 0 0 9 0 】

利用者は、提示された商取引情報から取引内容を確認し（ステップ S 6 0 4）、取引に同意する場合（ステップ S 6 0 4 : Y）、利用者端末 4 0 0 a が備える手書きサイン入力部 3 0 を介して手書きサイン欄にサインを手書き入力する（ステップ S 6 0 5）。

#### 【 0 0 9 1 】

手書きサイン入力部 3 0 は手書き入力したサインから電子サインデータを生成し、携帯端末 4 0 0 a から無線電話回線などのネットワーク 3 0 0 を通じて、電子サイン管理サーバ 1 0 0 a に対して直接送信する（ステップ S 6 0 6）。なお



、商取引情報は、利用者端末 4 0 0 a が電子サインデータとともに電子サイン管理サーバ 1 0 0 a に対して送信しても良く、また、決済機関のサーバ 2 0 0 a から電子サイン管理サーバ 1 0 0 a に対して送信しても良い。

【0 0 9 2】

なお、電子サイン管理サーバ 1 0 0 a における処理、つまり、利用者確認部 1 5 4 による利用者に対する利用者認証是非の利用者確認処理（ステップ S 6 0 7）、電子サインデータ要約処理部 1 5 2 による電子サインデータからの要約情報の生成（ステップ S 6 0 8）、電子透かし情報取得部 1 5 1 による付加情報の取得（ステップ S 6 0 9）、電子透かし付与処理部 1 5 3 による電子透かし付き電子サインデータの生成処理（ステップ S 6 1 0）に関しては、実施形態 1 の図 4 のフローチャートの処理と同様で良い。

【0 0 9 3】

最後に、電子サイン管理サーバ 1 0 0 a は、商取引における何らかのトラブルに備えるべく、電子透かし付き電子サインを商取引管理データ格納部 1 6 0 に登録し、さらに、電子サイン管理サーバ 1 0 0 a はデータ送受信部 1 1 0 を介して、生成した電子透かし付き電子サインデータを業者端末 1 0 a に送信し、商取引データ格納部 5 0 に格納する（ステップ S 6 1 1）。

【0 0 9 4】

以上が、本実施形態 2 の電子商取引システムおよび方法の処理の流れである。もちろん、上記処理の流れは一例であり、本発明の技術思想の及ぶ範囲において他の処理の流れとすることも可能である。

【0 0 9 5】

上記構成による電子商取引システムおよび方法とすることにより、利用者が保持する携帯端末 4 0 0 a を用いて電子サイン管理サーバ 1 0 0 a に対して直接電子サインデータを送信することができ、悪意の業者によるサインの盗用や複製といった不正行為に対するセキュリティ強度がさらに向上する。

【0 0 9 6】

（実施形態 3）

実施形態 3 の電子商取引システムおよび電子商取引方法を図を参照しつつ説明

する。本実施形態 3 は、電子透かし付与部を第 3 者機関に設けた構成ではなく、利用者端末に設ける構成としたものである。

【0097】

図 7 は、実施形態 3 の電子商取引システムの構成例を示すブロック図である。

【0098】

図 7 において、決済機関のサーバ 200b、ネットワーク 300 の諸構成要素は実施形態 1 で説明した図 1 と同様であるが、電子サイン管理サーバ 100 に相当する部分は設けられていない構成となっている。業者端末 10b は利用者識別情報読み取り部 20、業者端末の制御部 40、商取引データ格納部 50、データ送受信部 60 を備えている。利用者の携帯端末 400b は、手書きサイン入力部 30 および商取引情報提示部 31 に加え、電子透かし付与部 150 と電子透かし付き電子サインデータ格納部 160 を備えた構成となっている。なお、各要素は実施形態 1 と同様であるのでここでの説明は省略する。

【0099】

図 7 の構成によれば、電子透かし付与部 150 が利用者端末 400b に設けられているので、実施形態 1 や実施形態 2 の構成により必要となる電子透かし付与処理に対する利用者確認を不要とすることができ、また、電子サイン管理サーバとのやり取りも不要となる。さらに、電子透かし付加処理は利用者端末 400b において行うので、実施形態 1、実施形態 2 のように電子透かし付加処理前の利用者の確認を行う必要もなくなる。

【0100】

本実施形態 3 の電子商取引システムおよび方法の動作の流れを図 8 のフローチャートを参照しつつ説明する。

【0101】

まず、取引内容入力部 11 および利用者識別情報読み取り部 20 を介した取引内容に関する情報および利用者識別情報の入力処理（ステップ S801）、決済機関のサーバ 200b の商取引情報生成部 210 による商取引情報の生成（ステップ S802）、携帯端末 400b の商取引情報提示部 31 を介した商取引情報の利用者への提示（ステップ S803）、提示された商取引情報に対する利用者

による確認の是非（ステップ S 8 0 4）、利用者端末 4 0 0 b が備える手書きサイン入力部 3 0 を介した手書きサインの入力（ステップ S 8 0 5）、手書きサイン入力部 3 0 から生成された電子サインデータの電子サイン管理サーバ 1 0 0 b への送信（ステップ S 8 0 6）は実施形態 2 に示した図 6 のフローチャートに示したステップ S 6 0 1 とステップ S 6 0 6 の処理と同様である。なお、本実施形態 3 では、ステップ S 6 0 7 の利用者確認部 1 5 4 による利用者確認処理は実行されない。

#### 【 0 1 0 2 】

次に、利用者端末 4 0 0 b は、電子サインデータ要約処理部 1 5 2 により電子サインデータから要約情報を生成し（ステップ S 8 0 7）、電子透かし情報取得部 1 5 1 が今回の取引内容を特定する商取引識別子や要約情報などを電子透かし情報として取得し（ステップ S 8 0 8）、電子透かし付与処理部 1 5 3 が非公開のアルゴリズムにより電子サインデータに対して電子透かしとして埋め込み、電子透かし付き電子サインデータを生成する（ステップ S 8 0 9）。

#### 【 0 1 0 3 】

利用者端末 4 0 0 b は、生成した電子透かし付き電子サインデータを業者端末 1 0 b に送信し、商取引データ格納部 5 0 に格納する（ステップ S 8 1 0）。

#### 【 0 1 0 4 】

以上が、本実施形態 3 の電子商取引システムおよび方法の処理の流れである。もちろん、上記処理の流れは一例であり、本発明の技術思想の及ぶ範囲において他の処理の流れとすることも可能である。

#### 【 0 1 0 5 】

上記構成による電子商取引システムおよび方法とすることにより、電子透かし付与部が利用者端末に設けられているので、電子透かし付与処理に対する利用者確認を不要とすることができる。

#### 【 0 1 0 6 】

##### （実施形態 4）

実施形態 4 の電子商取引システムおよび電子商取引方法を図を参照しつつ説明する。本実施形態 4 は、サイン認証部 1 7 0 を追加した構成としたものである。

【0107】

図9は、実施形態4の電子商取引システムの構成例を示すブロック図である。

【0108】

図9において、業者端末10c、決済機関のサーバ200c、ネットワーク300、利用者の携帯端末400cの諸構成要素は実施形態1で説明した図1と同様であるが、電子サイン管理サーバ100cは、サイン認証部170を備えている構成となっている。なお、サイン認証部170以外の各要素は実施形態1と同様であるのでここでの説明は省略する。

【0109】

サイン認証部170は、利用者から入力された手書きサインが真正のサインであるか否かを認証する部分である。サイン認証部170は以下の構成要素を備えている。

【0110】

登録サイン格納部171は、あらかじめ利用者がクレジットカード生成時などに提供した利用者の真正サインを登録電子サインデータとして格納しておく部分である。ここでは実施形態1で説明した場合と同様、電子データとして登録保持されるものとする。

【0111】

サイン照合部172は、登録サイン格納部171に格納されている登録電子サインデータと、手書きサイン入力部30から入力された利用者の電子サインデータをマッチングし、照合処理する部分である。システムに要求される照合精度に応じて、最終的な筆跡形状のみならず、利用者の書き順、筆圧、筆記速度など多様な情報を用いて照合処理を行い、入力されたサインが真正であるか否かの情報を出力する。

【0112】

このサイン認証部170を設けた構成によれば、登録されている真正の電子サインデータと、商取引において手書きサイン入力部30から入力された利用者の電子サインデータをマッチングすることができ、利用者認証を高いセキュリティレベルで行うことができる。従来は業者自身が店頭において今回手書きされたサ

インと利用者カードの裏面などに書かれたサインとを目視により照合していたが、より正確かつ高いセキュリティによりサインの照合を行うことができる。

#### 【0113】

本実施形態4の電子商取引システムおよび方法の動作の流れを図10のフローチャートを参照しつつ説明する。

#### 【0114】

まず、取引内容入力部11および利用者識別情報読み取り部20を介した取引内容に関する情報および利用者識別情報の入力処理（ステップS1001）、決済機関のサーバ200cの商取引情報生成部210による商取引情報の生成（ステップS1002）、携帯端末400cの商取引情報提示部31を介した商取引情報の利用者への提示（ステップS1003）、提示された商取引情報に対する利用者による確認の是非（ステップS1004）、利用者端末400cが備える手書きサイン入力部30を介した手書きサインの入力（ステップS1005）、手書きサイン入力部30から生成された電子サインデータの電子サイン管理サーバ100cへの送信（ステップS1006）は実施形態2に示した図6のフローチャートに示したステップS601とステップS606の処理と同様である。

#### 【0115】

本実施形態4の電子商取引システムおよび方法では、サイン認証処理を実行する。電子サイン管理サーバ100cは、データ送受信部110を介して電子サインデータと商取引情報を受け取り、商取引情報の利用者識別情報から登録サイン格納部171に格納されている利用者の登録サインデータを検索し、サイン照合部172において登録電子サインデータと利用者の電子サインデータをマッチングし、照合処理する（ステップS1007）。

#### 【0116】

次に、利用者確認部154により、利用者に対して直接、利用者認証しても良いか確認する（ステップS1008）。つまり、該商取引における電子透かし付き電子サインデータ生成の是非の確認を行う。

#### 【0117】

利用者からの確認が得られれば（ステップS1008：Y）、電子透かし付加

処理に移行する。電子サイン管理サーバ 1 0 0 c は、電子サインデータ要約処理部 1 5 2 により電子サインデータから要約情報を生成し（ステップ S 1 0 0 9）、電子透かし情報取得部 1 5 1 が今回の取引内容を特定する商取引識別子や要約情報などを電子透かし情報として取得し（ステップ S 1 0 1 0）、電子透かし付与処理部 1 5 3 が非公開のアルゴリズムにより電子サインデータに対して電子透かしとして埋め込み、電子透かし付き電子サインデータを生成する（ステップ S 1 0 1 1）。

#### 【 0 1 1 8 】

電子サイン管理サーバ 1 0 0 c は、生成した電子透かし付き電子サインデータを業者端末 1 0 c に送信し、商取引データ格納部 5 0 に格納する（ステップ S 1 0 1 2）。

#### 【 0 1 1 9 】

以上が、本実施形態 4 の電子商取引システムおよび方法の処理の流れである。もちろん、上記処理の流れは一例であり、本発明の技術思想の及ぶ範囲において他の処理の流れとすることも可能である。

#### 【 0 1 2 0 】

以上、本実施形態 4 の電子商取引システムおよび方法によれば、電子サイン管理サーバ 1 0 0 c による利用者認証を行う処理が実行されないので、商取引の処理内容を低減することができ、処理の効率化を図ることができる。

#### 【 0 1 2 1 】

##### （実施形態 5）

本実施形態 5 の電子商取引システムおよび方法は、実運用上の使い勝手を向上する工夫を加えたものである。現在、一部のクレジットカードの運用や、一部のデビットカードの運用において、一定額以下の小額取引については、店舗内での手続時間の短縮化や、利用者の手続負担軽減のため、取引伝票に対するサインを省略するという運用が見られる。本実施形態 5 の電子商取引システムおよび方法は、一定額以下の小額取引などについては手書きサイン入力を省略し、電子透かし付き電子サインデータの生成に代え、電子透かし付き電子サイン省略商取引情報を生成して決済を完了するものである。

## 【 0 1 2 2 】

図 1 1 は、実施形態 5 の電子商取引システムの構成例を示すブロック図である。図 1 1 において、決済機関のサーバ 2 0 0 d は、手書きサイン省略可否判定部 2 2 0 を備えている。手書きサイン省略可否判定部 2 2 0 は、業者識別情報、利用者識別情報、決済金額情報など商取引情報に基づいて、手書きサインによる利用者認証処理を省略するか否かを判断する部分である。例えば、業者識別情報に基づいて業者の別に応じてサインを省略する運用を認めるか否かを調整したり、利用者識別情報に基づいて利用者の別に応じてサインを省略する運用を認めるか否かを調整したり、さらに、決済金額情報に基づいて、決済金額の大きさに応じてサインを省略する運用を認めるか否かを調整することができる。手書きサイン省略可否判定部 2 2 0 により手書きサインの省略が認められた場合、手書きサイン入力部 3 0 による電子サインデータ読み取りと、電子透かし付与部 1 5 0 による電子透かし付き電子サインデータの生成が省略され、商取引データ格納部 5 0 に利用者識別情報と商取引情報を格納するものである。

## 【 0 1 2 3 】

なお、図 1 1 のその他の構成要素は実施形態 1 の図 1 や実施形態 2 の図 5 のものと同様で良い。ここでは決済機関のサーバ 2 0 0 d 以外の構成は図 1 のものと同様の例とする。なお、ここでのその他の各要素の説明は省略する。

## 【 0 1 2 4 】

図 1 2 は、実施形態 5 の電子商取引システムおよび方法の処理の流れの例を示すフローチャートである。

## 【 0 1 2 5 】

まず、取引内容入力部 1 1 および利用者識別情報読み取り部 2 0 を介した取引内容に関する情報および利用者識別情報の入力処理（ステップ S 1 2 0 1）、決済機関のサーバ 2 0 0 d の商取引情報生成部 2 1 0 による商取引情報の生成（ステップ S 1 2 0 2）は実施形態 1 に示した図 4 のフローチャートに示したステップ S 4 0 1 とステップ S 4 0 2 の処理と同様である。

## 【 0 1 2 6 】

次に、決済機関のサーバ 2 0 0 d は、手書きサイン省略可否判定部 2 2 0 によ

り、業者識別情報、利用者識別情報、決済金額情報など商取引情報に基づいて手書きサインによる利用者認証処理を省略するか否かを判定する（ステップ S 1 2 0 3）。

#### 【 0 1 2 7 】

手書きサインによる利用者認証処理を省略する場合（ステップ S 1 2 0 3 : Y）、実施形態 1 において実行されるステップ S 4 0 4 ～ステップ S 4 1 1、または、実施形態 2 において実行されるステップ S 6 0 4 ～ステップ S 6 1 1、または、実施形態 3 において実行されるステップ S 8 0 4 ～ステップ S 8 1 0、または、実施形態 4 において実行されるステップ S 1 0 0 4 ～ステップ S 1 0 1 2 までの処理が省略され、電子透かし付与部 1 5 0 は、商取引情報に対して、電子透かし付き電子サインの埋め込みを省略し（ステップ S 1 2 0 4）、商取引データ格納部 5 0 に利用者識別情報と商取引情報を格納する。（ステップ S 1 2 0 5）

#### 【 0 1 2 8 】

以上、本実施形態 5 による電子商取引システムおよび方法は、一定額以下の小額取引などについては手書きサイン入力を省略して決済を完了することができ、店舗内での手続時間の短縮化や、利用者の手続負担軽減を図ることができる。

#### 【 0 1 2 9 】

##### （実施形態 6）

実施形態 6 の電子商取引システムおよび方法は、事後的に商取引における何らかのトラブルにより、電子サインの正当性が問題となった場合に、電子サインが正当なものであるか不正なものかを確認する処理を実行するものである。

#### 【 0 1 3 0 】

図 1 3 が本実施形態 6 の電子サインの正当性を確認するためのシステム構成例を示すブロック図である。9 0 0 が電子サイン検証装置である。電子サイン検証装置 9 0 0 は、商取引情報取得部 9 1 0、電子透かし付き電子サインデータ取得部 9 2 0、改ざんチェック部 9 3 0、商取引識別子抽出部 9 4 0、商取引情報検索部 9 5 0、商取引情報格納部 9 5 1、検証部 9 6 0 を備えている。

#### 【 0 1 3 1 】



商取引情報取得部 9 1 0 および電子透かし付き電子サインデータ取得部 9 2 0 は、検証すべき商取引の結果として保存されている商取引情報および電子透かし付き電子サインデータを取得する部分である。取得された商取引情報は検証部 9 6 0 に渡され、電子透かし付き電子サインデータは後述する処理実行のため改ざんチェック部 9 3 0 に渡される。

#### 【 0 1 3 2 】

改ざんチェック部 9 3 0 は、商取引に用いられた電子サインデータに改ざんがないかをチェックする部分である。改ざんチェック部 9 3 0 は電子サインデータに埋め込まれている電子透かし情報を調べることにより電子サインデータの改ざんの有無を判定する。この実施形態 6 では特に電子サインの要約情報を調べることにより電子サインデータの改ざんの有無を判別するものとする。電子サインデータに対して何らかの改ざんを行った場合、付されている要約情報と対応しなくなってしまうので改ざんの有無を判別することが可能となる。つまり、電子サイン自体が不正に書き換えられている場合は、要約情報が異なるものとなり、改ざんチェック部において電子サインデータへの不正行為が検証できるわけである。改ざんチェック部 9 3 0 は、改ざんを検出した場合は検証部 9 6 0 に送り、検証部 9 6 0 は不正検証結果を出力する。改ざんチェック部 9 3 0 が改ざんを検出しない場合は、商取引識別子抽出部 9 4 0 へ電子透かし付き電子サインデータを渡す。

#### 【 0 1 3 3 】

商取引識別子抽出部 9 4 0 は、電子透かし付き電子サインデータから商取引識別子を抽出する部分である。

#### 【 0 1 3 4 】

商取引情報検索部 9 5 0 は、商取引識別子抽出部 9 4 0 が抽出した商取引識別子を検索キーとして商取引情報格納部 9 5 1 に格納されている商取引情報を検索する部分である。なお、商取引情報格納部 9 5 1 は、事前に電子サイン検証装置 9 0 0 に用意されている真正取引情報が蓄積されたデータベースであり、例えば商取引時に電子サイン管理サーバなどに格納された商取引情報を取り寄せて該真正の商取引情報を格納したデータベースである。実施形態 1 などで示した電子サ

イン管理サーバ 1 0 0 では商取引管理データ格納部 1 6 0 において格納された商取引情報に相当するデータベースであれば良い。なお、この実施形態 6 および図 1 3 のシステム構成例においては電子サインの正当性を確認するシステム 9 0 0 が商取引情報格納部 9 5 1 を含んだ構成としているが、商取引情報格納部 9 5 1 に相当するものをシステム 9 0 0 内に持たず、決済機関など第三者機関が格納しているデータベースを利用する構成であっても良い。

#### 【 0 1 3 5 】

検証部 9 6 0 は、商取引情報取得部 9 1 0 から入力された商取引情報、つまり、検証すべき商取引情報と、商取引情報検索部 9 5 0 により検索された商取引情報、つまり、電子透かし付き電子サインデータから抽出した当該電子サインに対応する商取引情報の両者を比較・照合する部分である。この両者の比較・照合において両者が一致すれば当該電子透かし付き電子サインデータは真正のもので対応する商取引情報に対して正当なものであったことが検証され、両者が一致しない場合は、逆に当該電子透かし付き電子サインデータは対応する商取引情報に対して正当なものではないことが検証される。つまり、電子サイン自体は過去に正当に利用者により書き込まれたものであるが、他の架空取引に不正に流用されたものであるので対応する商取引情報が異なるものとなる。

#### 【 0 1 3 6 】

本実施形態 6 の電子商取引システムおよび方法によれば、電子サイン偽造、電子サイン流用いずれの不正に対してもその正当性を検証することができる。

#### 【 0 1 3 7 】

##### (実施形態 7)

本発明の電子透かし付き電子サインを用いた電子商取引システムは、上記に説明した構成を実現する処理ステップを記述したプログラムをコンピュータ読み取り可能な記録媒体に記録して提供することにより、各種コンピュータを用いて構築することができる。本発明の電子透かし付き電子サインを用いた電子商取引システムを実現する処理ステップを備えたプログラムを記録した記録媒体は、図 1 4 に図示した記録媒体の例に示すように、CD-ROM 1 0 0 2 やフレキシブルディスク 1 0 0 3 等の可搬型記録媒体 1 0 0 1 だけでなく、ネットワーク上にあ

る記録装置内の記録媒体 1 0 0 0 や、コンピュータのハードディスクや RAM 等の記録媒体 1 0 0 5 のいずれであっても良く、プログラム実行時には、プログラムはコンピュータ 1 0 0 4 上にローディングされ、主メモリ上で実行される。

【0 1 3 8】

【発明の効果】

本発明の電子透かし付き電子サインを用いた電子商取引システムによれば、本発明によれば、電子サインの利用により業者側あるいは第三者の悪意による電子サインの不正利用を防止できるため、カード取引によるサイン入力 of 電子化が可能となり、それによって利用者側の不正カード利用の防止や紙の取引伝票の保管コストなどの経費削減に効果がある。

【0 1 3 9】

また、利用者が保持する携帯端末に手書きサイン入力部を設ける構成として業者側の悪意による不正利用に対するセキュリティを高めることができる。

【0 1 4 0】

また、電子透かし付与を利用者端末側で実行して、処理ステップを低減し、処理効率を向上することができる。

【0 1 4 1】

また、電子透かし情報として、利用者識別情報や商取引情報などに加え、電子サインデータから生成した要約情報を用いることができ、改ざんの困難な電子透かし情報を用いることができる。

【図面の簡単な説明】

【図 1】 本発明の実施形態 1 の電子商取引システムの構成例を示すブロック図

【図 2】 (a) は電子サインの筆跡形状の例を示す図、(b) は座標点の列のデータとして表現された電子サインデータの例を示す図

【図 3】 連続する二つの座標点  $P_i$ ,  $P_{i+1}$  の間に、 $P_i$  と  $P_{i+1}$  を  $N:M$  に内分する座標点  $P_{i'}$  が埋め込まれる様子を模式的に表した図

【図 4】 実施形態 1 の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図 5】 本発明の実施形態 2 の電子商取引システムの構成例を示すブロック図

【図 6】 実施形態 2 の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図 7】 本発明の実施形態 3 の電子商取引システムの構成例を示すブロック図

【図 8】 実施形態 3 の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図 9】 本発明の実施形態 4 の電子商取引システムの構成例を示すブロック図

【図 1 0】 実施形態 4 の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図 1 1】 本発明の実施形態 5 の電子商取引システムの構成例を示すブロック図

【図 1 2】 実施形態 5 の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図 1 3】 本実施形態 6 の電子サインの正当性を確認するためのシステム構成例を示すブロック図

【図 1 4】 本発明の実施形態 6 の電子透かし付き電子サインを用いた電子商取引システムを実現する処理プログラムを格納した記録媒体の例を示す図

【図 1 5】 従来の電子商取引方法を組み合わせたシステム構築例を示す図

【符号の説明】

1 0, 1 0 a, 1 0 b, 1 0 c, 1 0 d 業者端末

1 1 取引内容入力部

2 0 利用者識別情報読み取り部

3 0 手書きサイン入力部

3 1 商取引情報提示部

4 0 制御部

5 0 商取引データ格納部

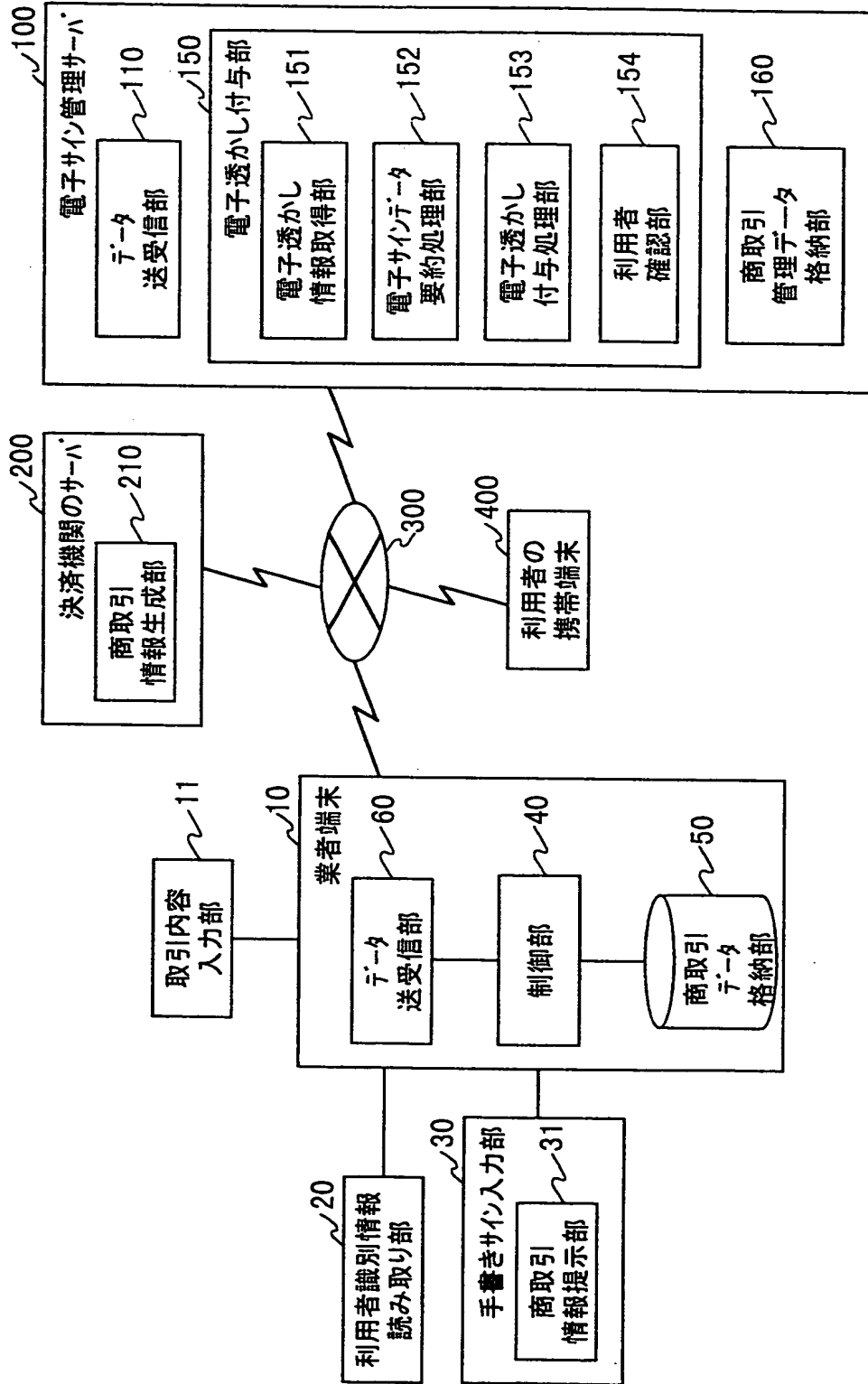
6 0 , 1 1 0 データ送受信部  
1 0 0 , 1 0 0 a , 1 0 0 b , 1 0 0 c 電子サイン管理サーバ  
1 4 0 利用者認証部  
1 5 0 電子透かし付与部  
1 5 1 電子透かし情報取得部  
1 5 2 電子サインデータ要約処理部  
1 5 3 電子透かし付与処理部  
1 5 4 利用者確認部  
1 6 0 商取引管理データ格納部  
1 7 0 サイン認証部  
1 7 1 登録サイン格納部  
1 7 2 サイン照合部  
2 0 0 , 2 0 0 a , 2 0 0 b , 2 0 0 c , 2 0 0 d 決済機関のサーバ  
2 1 0 商取引情報生成部  
2 2 0 手書きサイン省略可否判定部  
3 0 0 ネットワーク  
4 0 0 , 4 0 0 a , 4 0 0 b , 4 0 0 c 利用者の携帯端末  
9 0 0 電子サイン検証装置  
9 1 0 商取引情報取得部  
9 2 0 電子透かし付き電子サインデータ取得部  
9 3 0 改ざんチェック部  
9 4 0 商取引識別子抽出部  
9 5 0 商取引情報検索部  
9 5 1 商取引情報格納部  
9 6 0 検証部  
1 0 0 0 記録装置内の記録媒体  
1 0 0 1 可搬型記録媒体  
1 0 0 2 C D - R O M  
1 0 0 3 フレキシブルディスク

1 0 0 4    コンピュータ

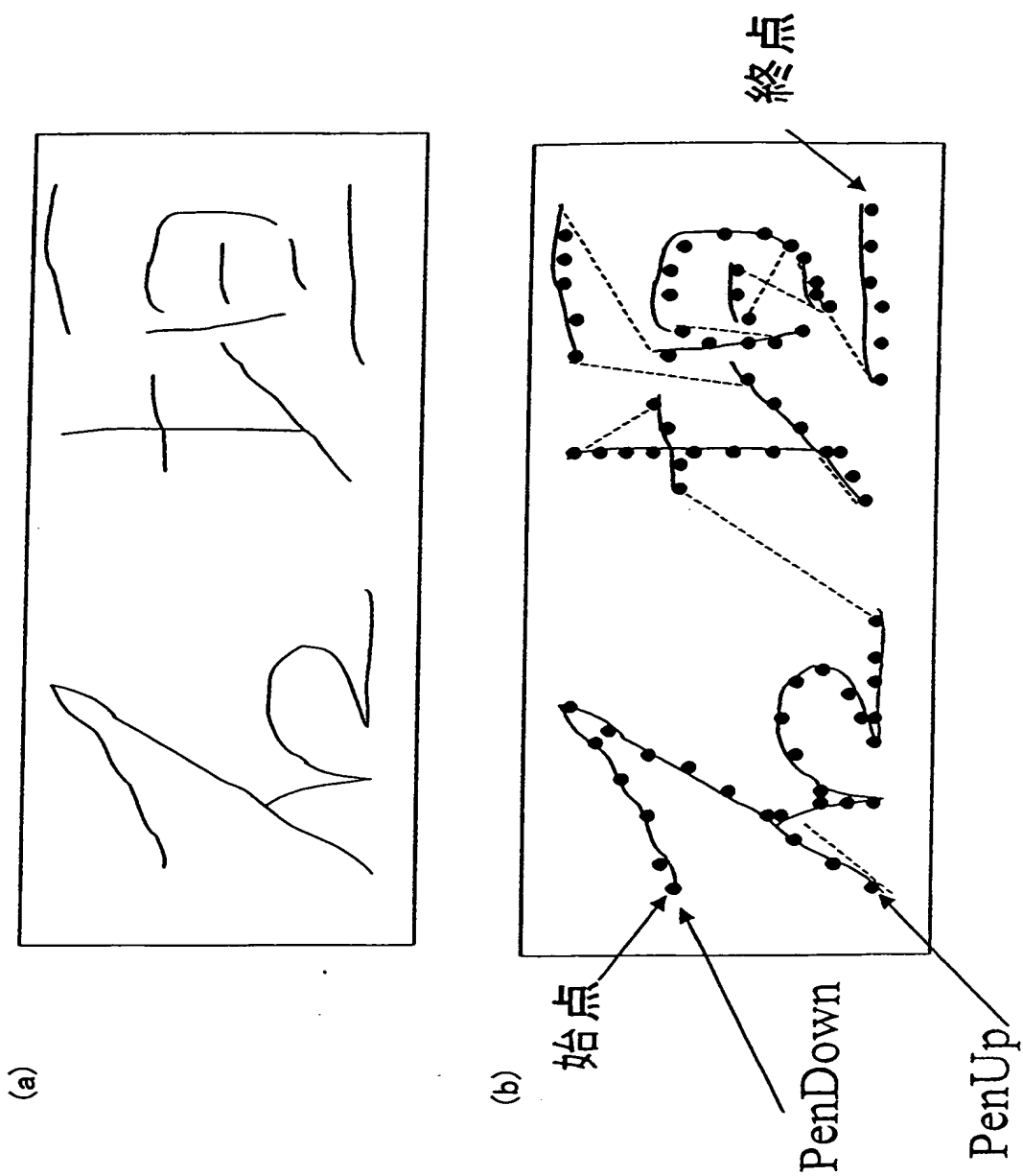
1 0 0 5    コンピュータのハードディスクやRAM等の記録媒体

【書類名】 図面

【図 1】

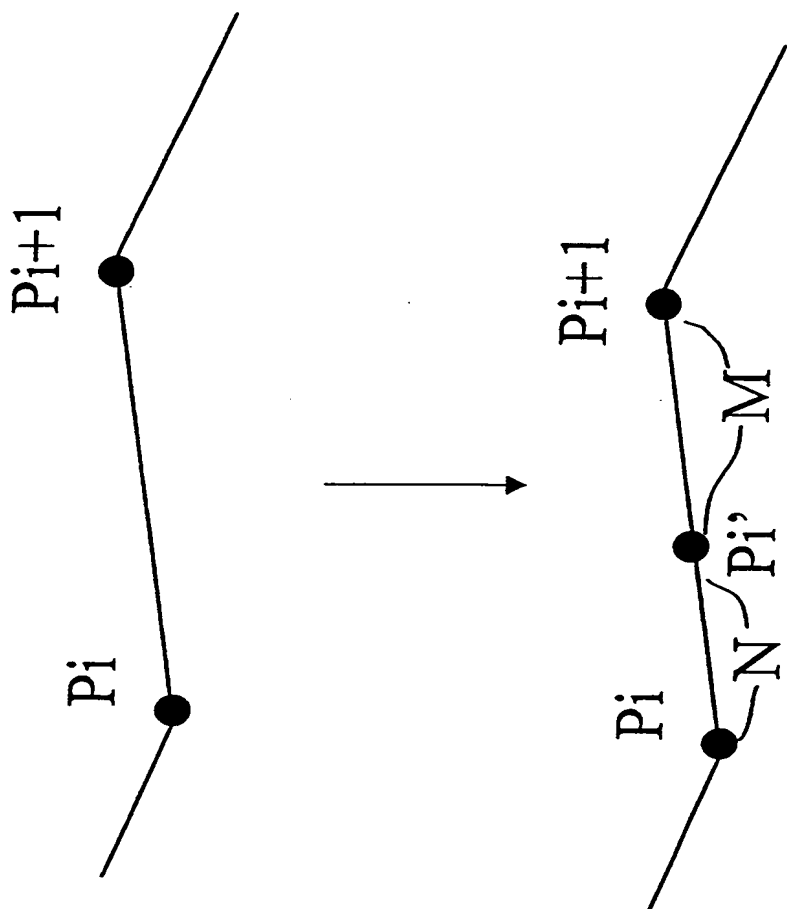


【図2】

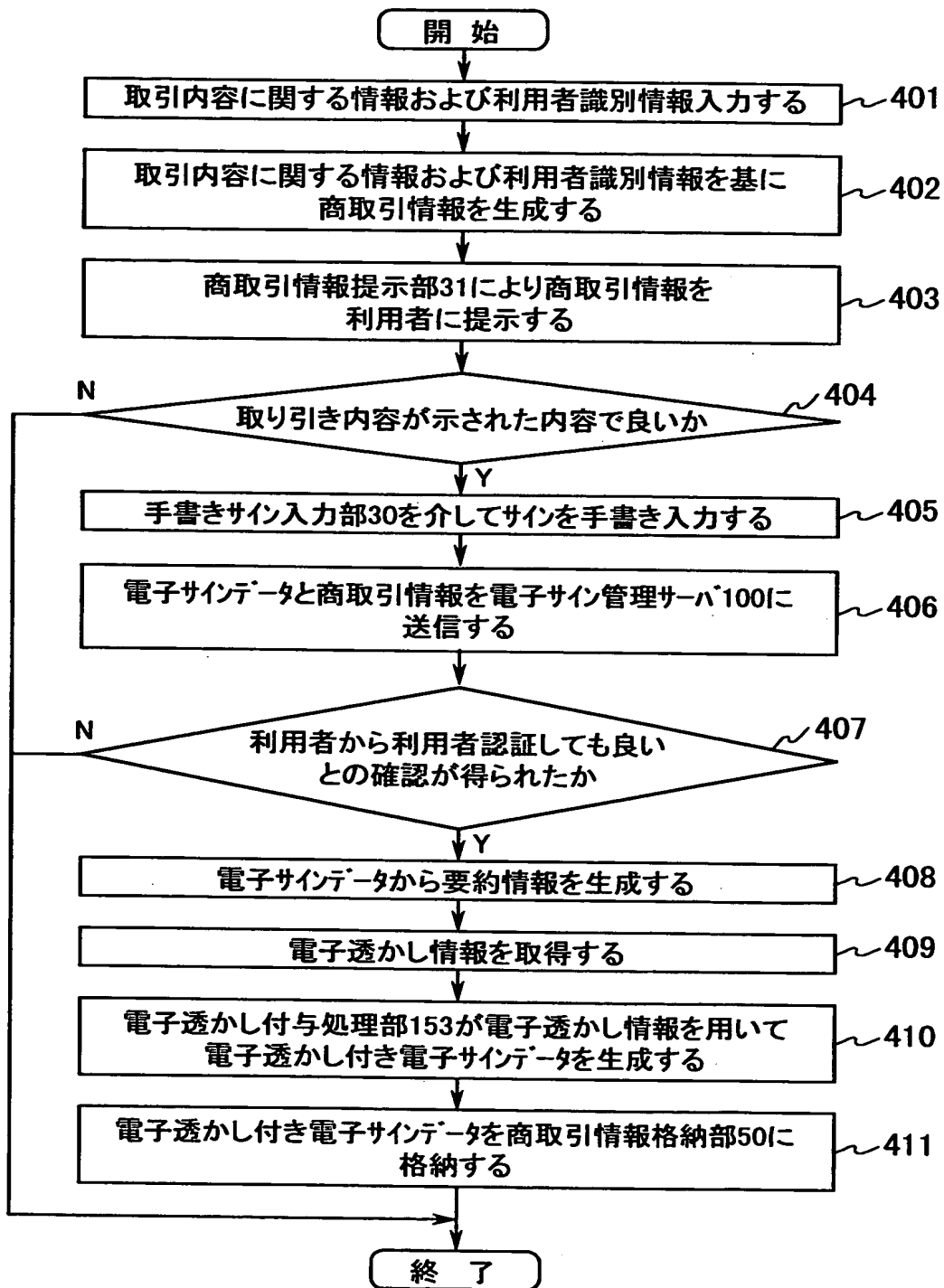




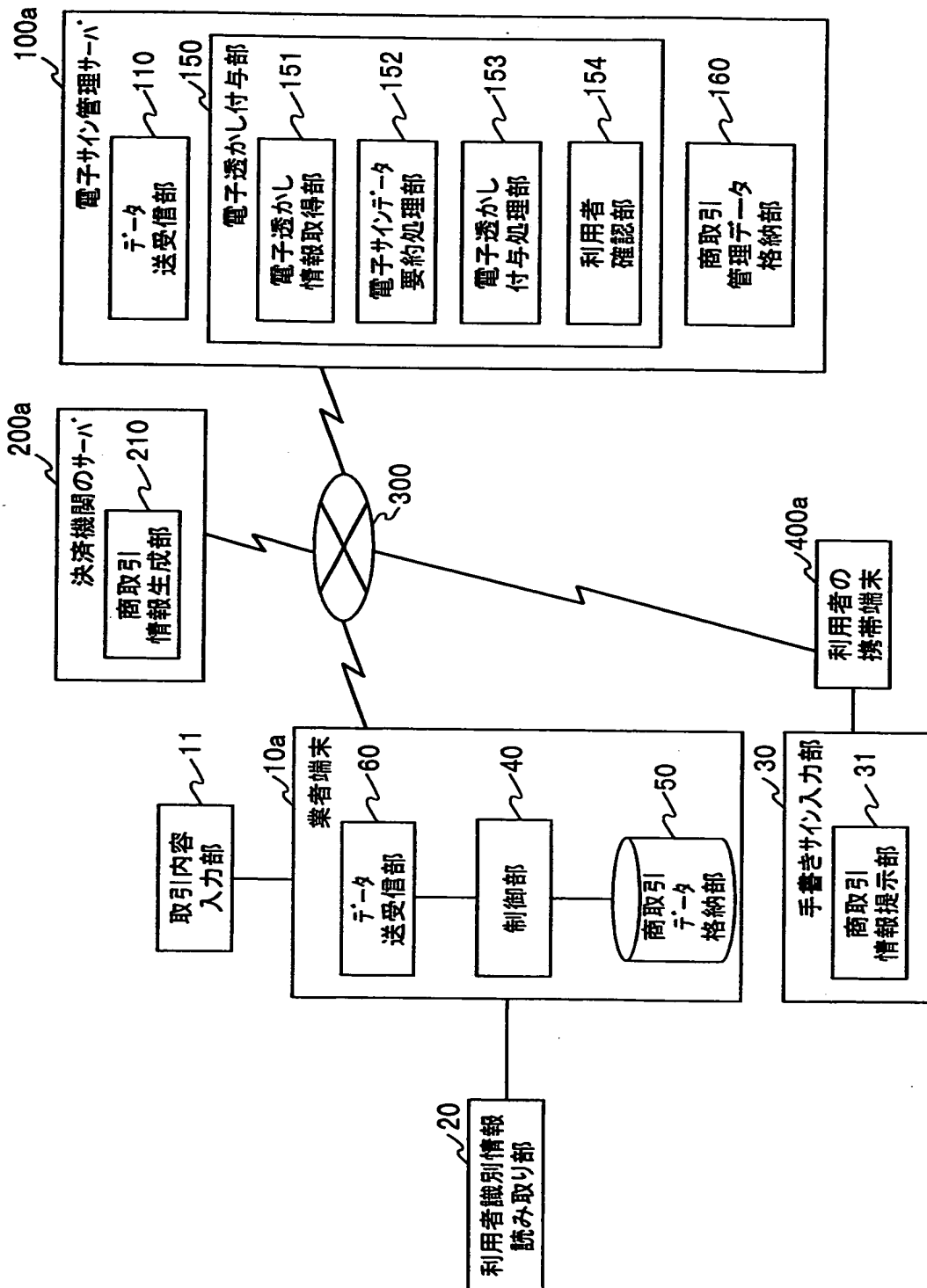
【図 3】



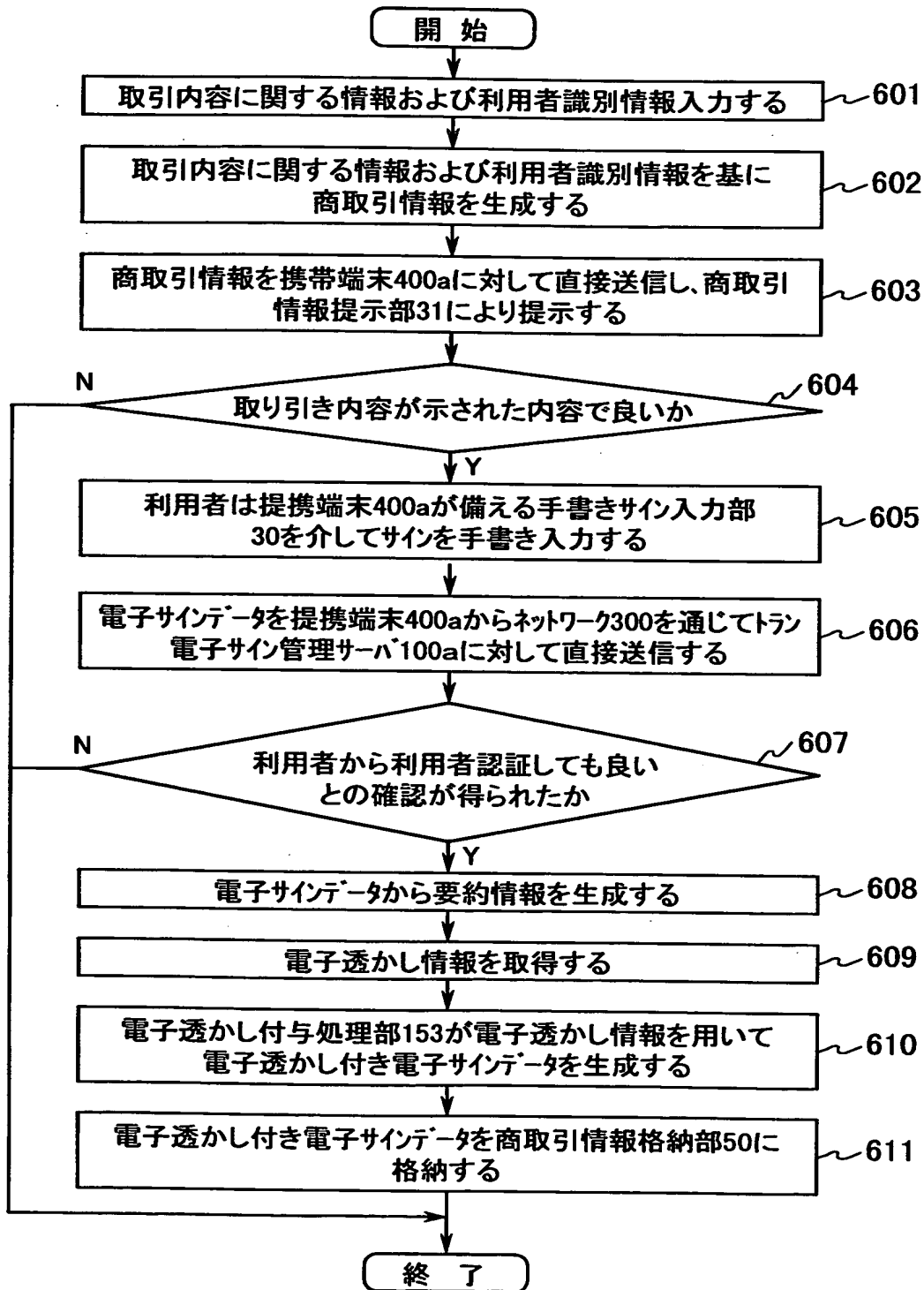
【図 4】



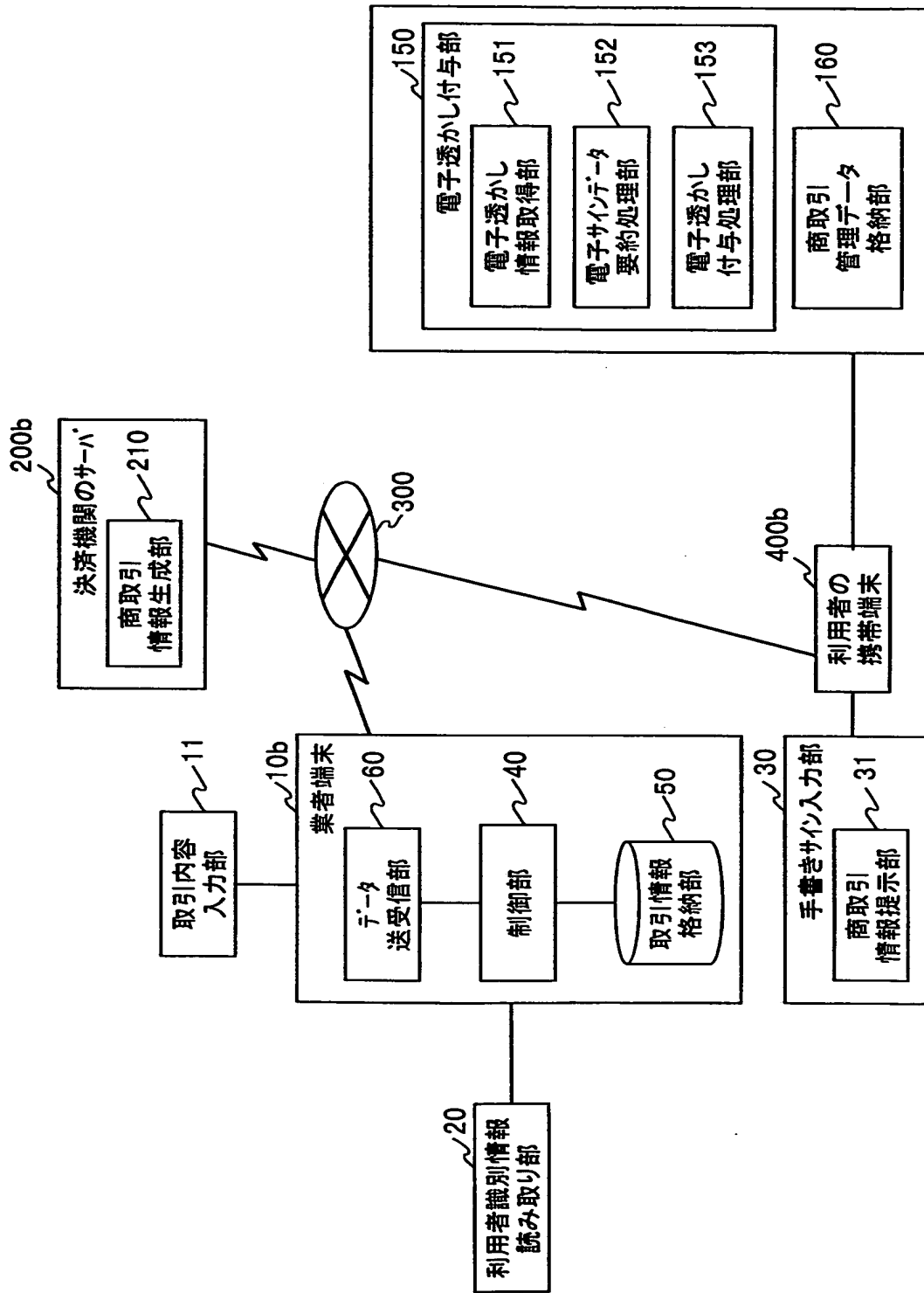
【図 5】



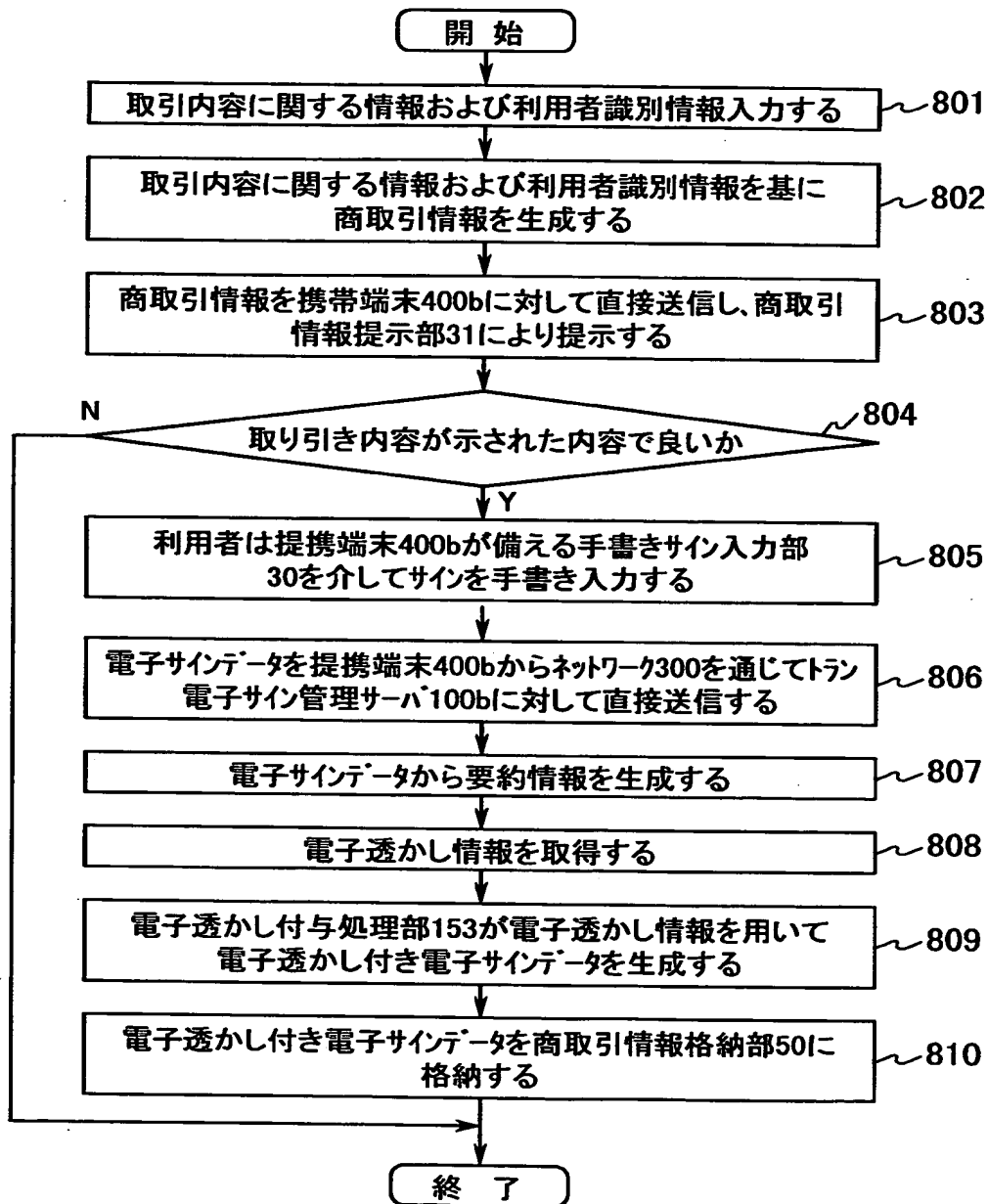
【図 6】



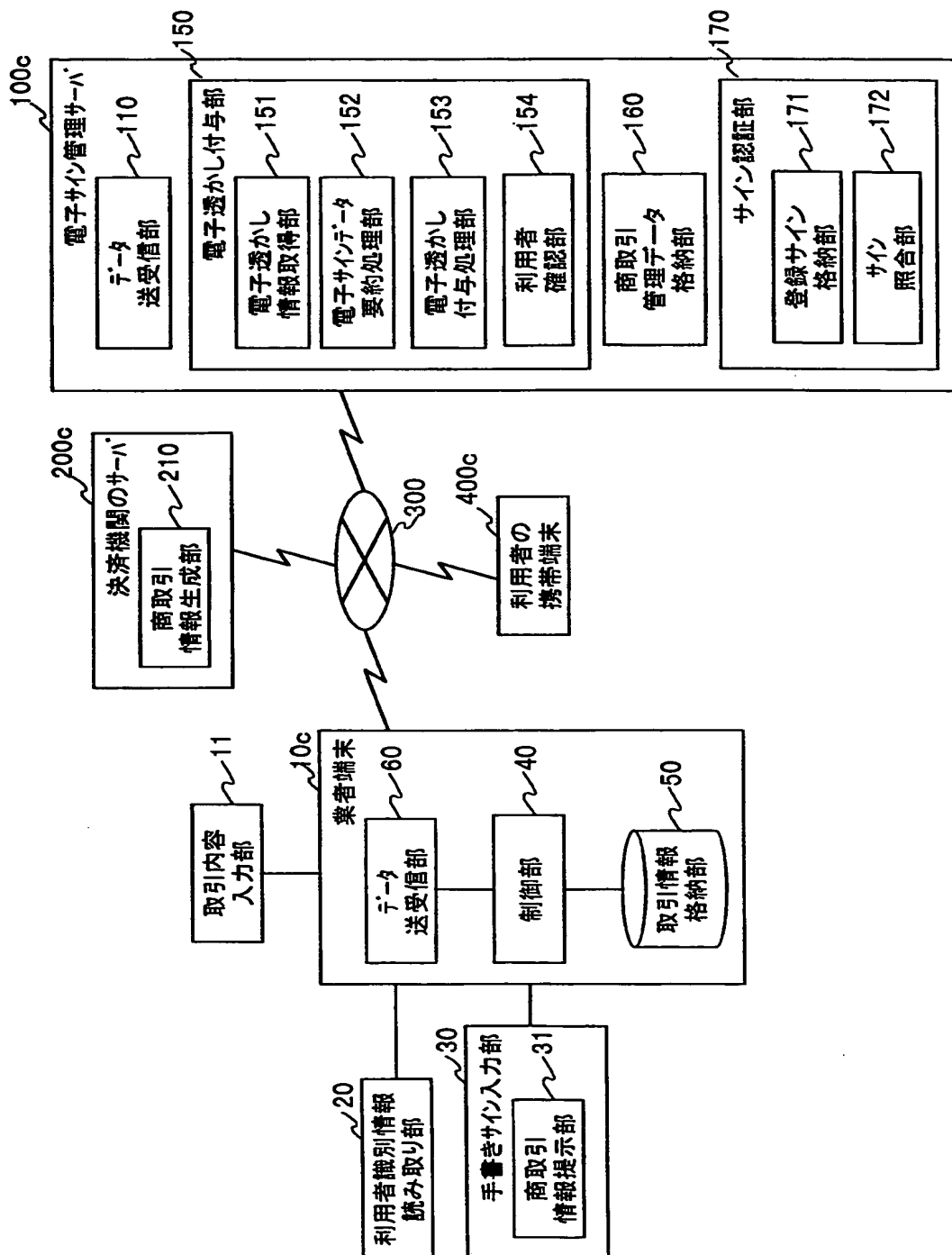
【図 7】



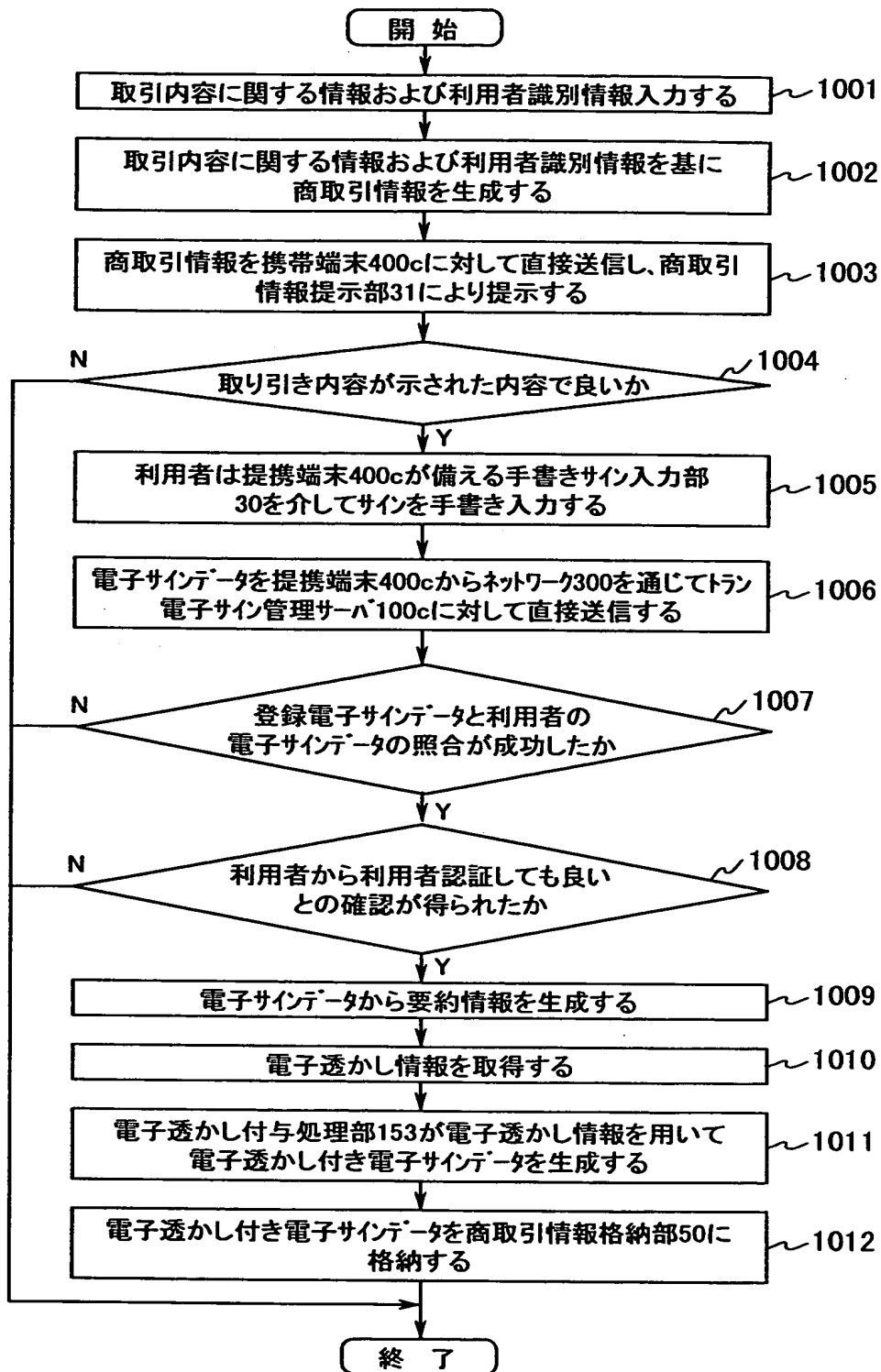
【図 8】



【図9】

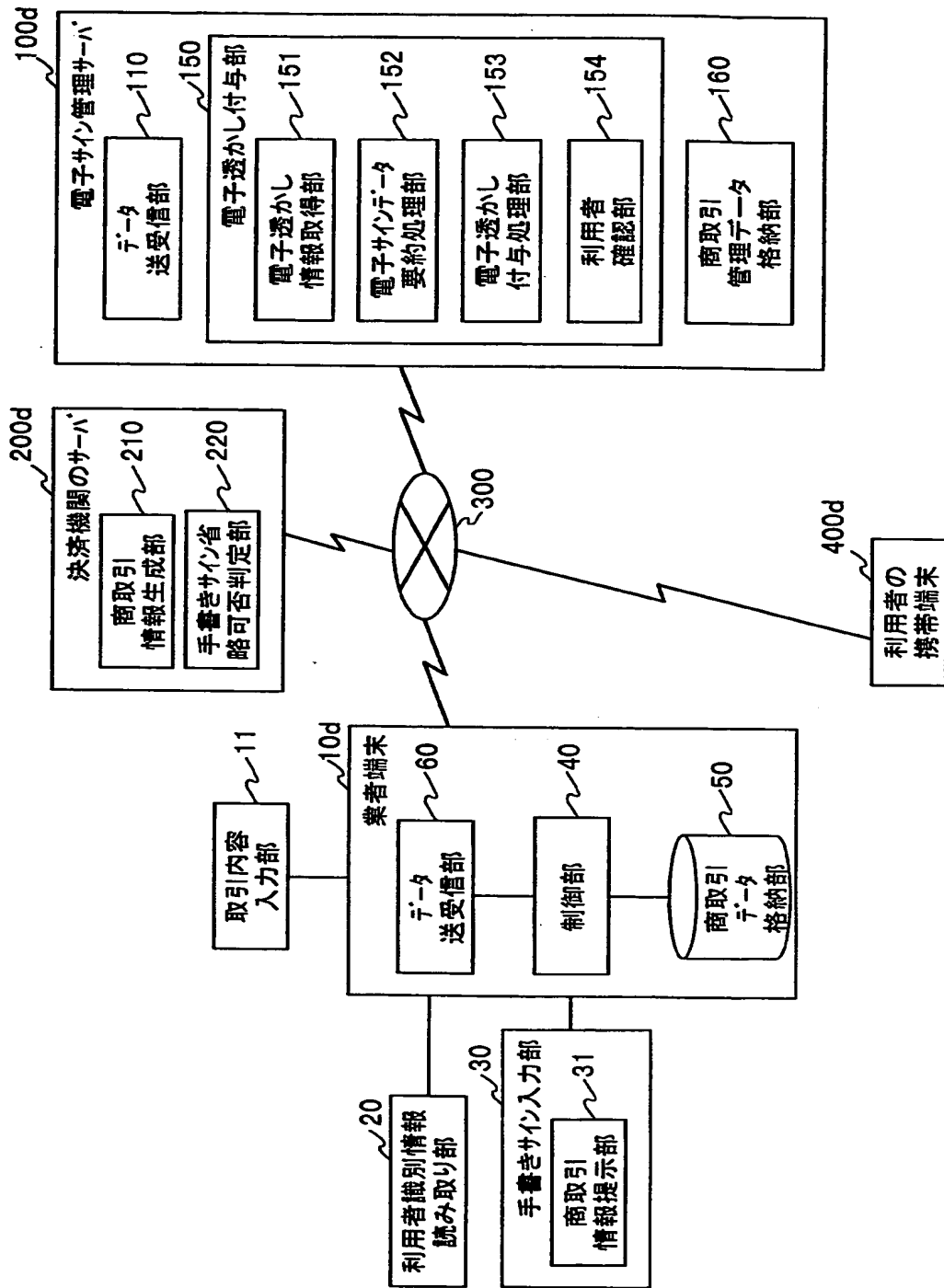


【図 10】

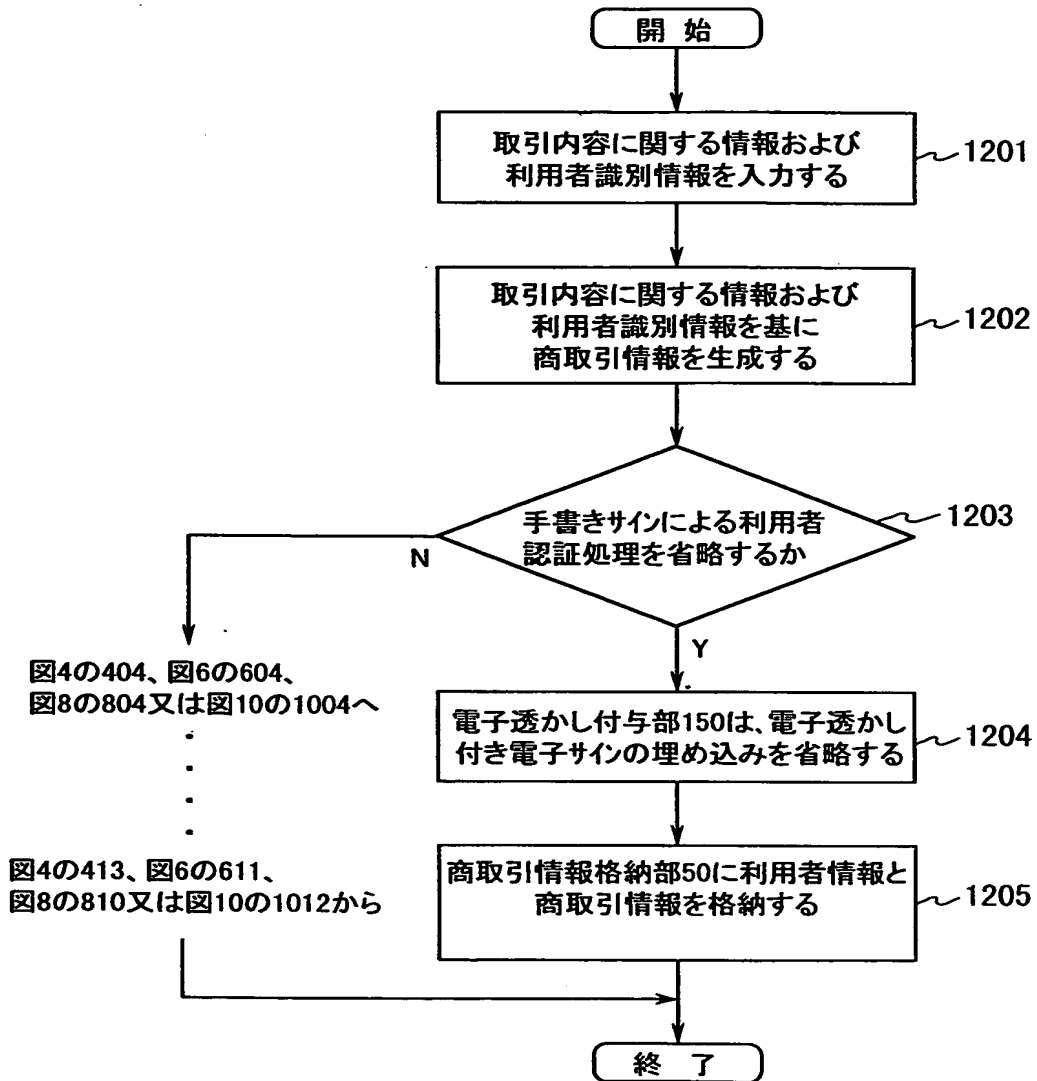




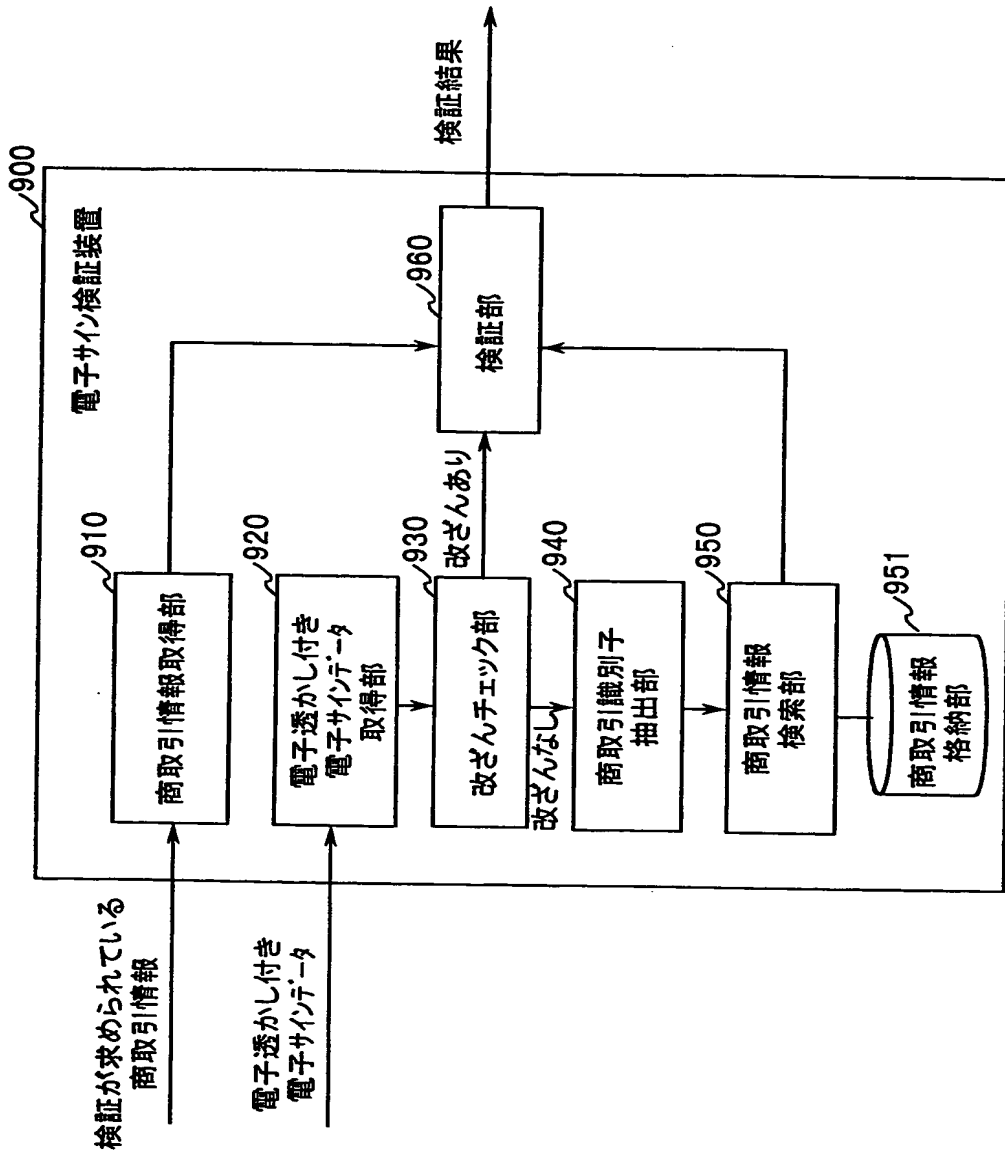
【図 11】



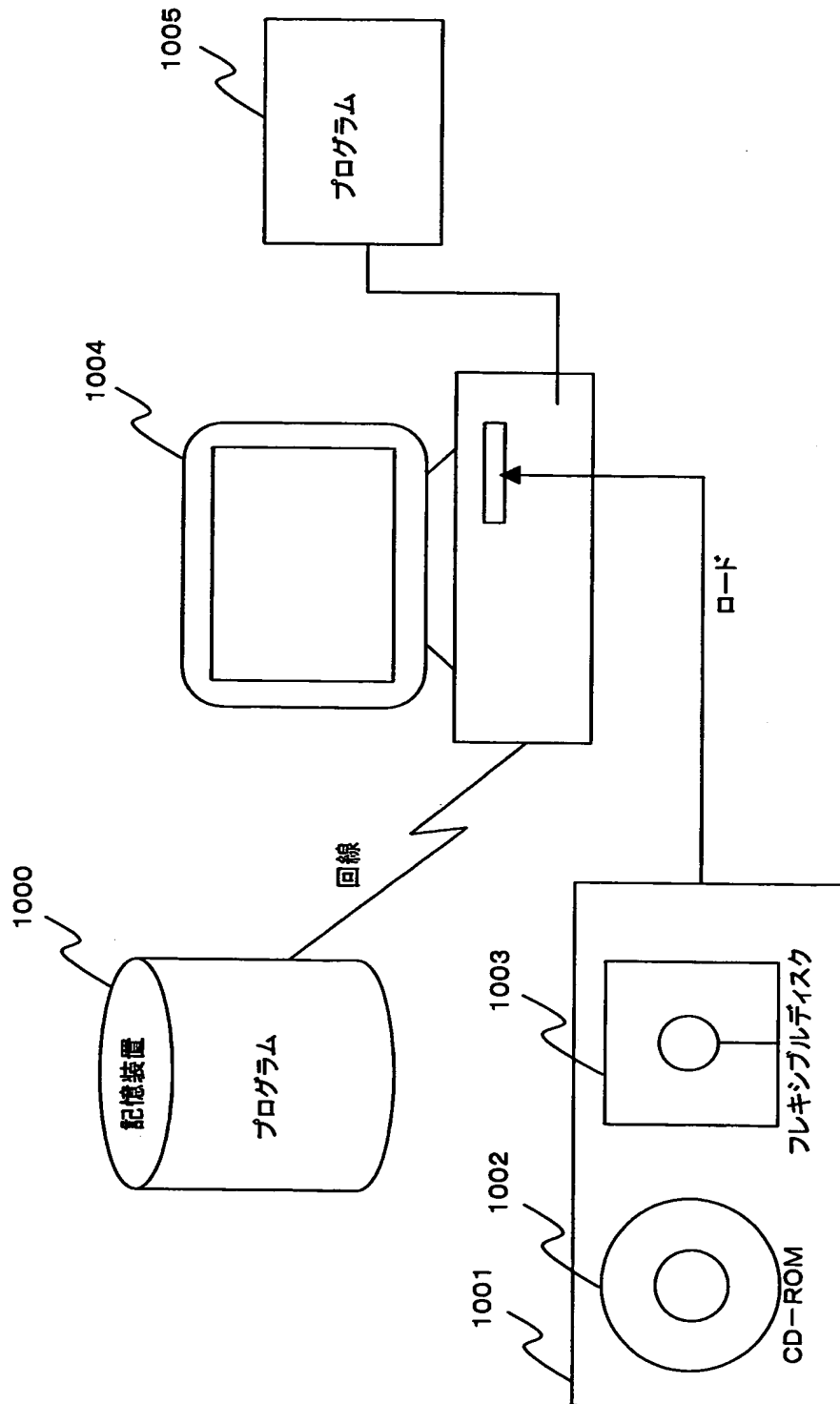
【図 12】



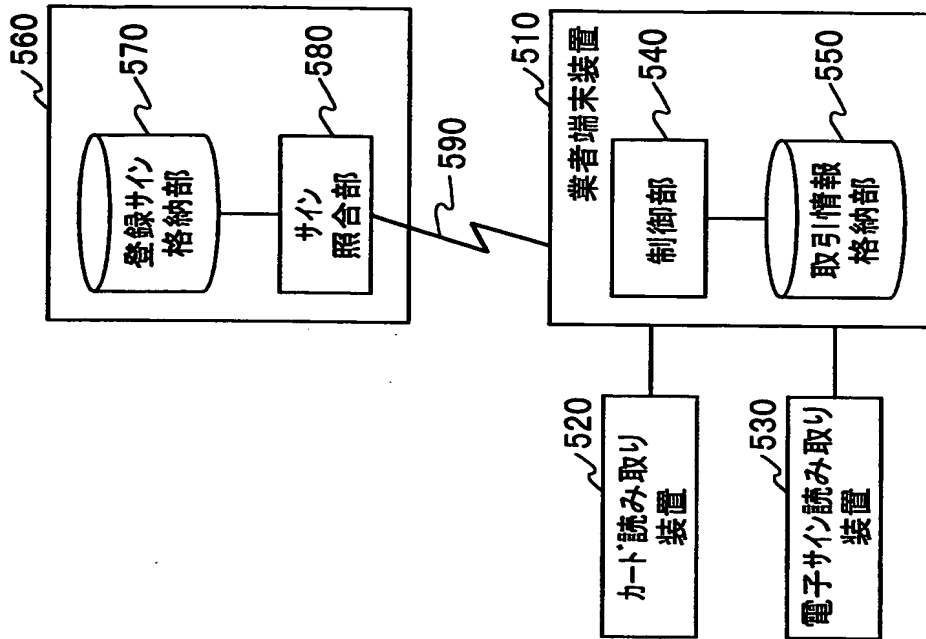
【図13】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 電子サインの取引業者による偽造、架空取引などへの流用を効果的に防止できる電子商取引システムおよび方法を提供する。

【解決手段】 取引内容入力部 1 1 と利用者識別情報読み取り部 2 0 から取引情報と利用者識別情報が入力され、決済機関のサーバ 2 0 0 に送られ、商取引情報生成部 2 1 0 により商取引情報が生成される。利用者は商取引情報提示部 3 1 を介して提示された取引内容を確認し手書きサイン入力部 3 0 からサインを入力する。電子サインデータと商取引情報は電子サイン管理サーバ 1 0 0 に送信され、サイン照合部 1 3 0 による電子サインデータの照合の後、電子サインデータの要約情報と取引内容を特定する商取引識別子とを電子透かし情報として付加し、電子透かし付き電子サインデータを生成する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号  
氏 名 富士通株式会社